



## POLITIQUE DE CONFIDENTIALITÉ

### Introduction

L'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) se conforme aux Lois et Règlements du Cameroun. Il s'agit notamment de : la Loi relative à la cybersécurité et à la cybercriminalité, la Loi sur le commerce électronique, la Loi régissant les communications électroniques, la Loi sur la protection des informations à caractère personnel, la Loi sur la protection du consommateur et les textes réglementaires subséquents, pour assurer la protection des informations à caractère personnel lorsqu'il est nécessaire de collecter ce type d'informations sur un individu qui sollicite l'obtention d'un certificat lui permettant d'effectuer les transactions électroniques sur un site sécurisé à l'aide de l'infrastructure nationale à clé publique. L'Agence se porte donc garant de la confidentialité des informations qu'elle aura collectées dans le cadre du Service de la certification. Dans ce cas, la politique de confidentialité est établie et exécutée ainsi qu'il suit:

### 1. Procédure de protection des informations confidentielles

L'ANTIC collecte les informations à caractère personnel lorsque le consommateur sollicite l'obtention d'un certificat pour effectuer des transactions électroniques, l'acquisition d'un nom de domaine, la sécurisation d'une de ses applications à l'aide de l'infrastructure à clé publique, devenir une autorité d'enregistrement ou lorsqu'il s'agit de compléter certaines informations nécessaires à l'émission d'un certificat ou utiles à d'autres services fournis par l'Agence.

#### A. Service de la certification ouvert au public

① Des informations à caractère personnel sont essentiellement collectées dans le strict respect des dispositions des Lois et Règlements de la République du Cameroun. Sont notamment visées, la Loi relative à la cybersécurité et à la cybercriminalité, la Loi régissant le commerce électronique, la Loi sur les communications électroniques, ainsi qu'il suit :

- Administration/Institution : Nom de l'Institution/Ministère/Université, Code Budgétaire, Nom du Président/Ministre/Recteur, Numéro de la CNI du Président/Ministre/Recteur, Nom du Mandataire, numéro de la CNI du Mandataire, période d'emploi, lettre donnant quitus au Mandataire pour faire la transaction au nom de l'Administration/Institution/Université, Informations sur l'utilisateur final du certificat (nom, numéro de la CNI, organisation, direction, téléphone (Bureau/Domicile/mobile), fax, e-mail) ;
- Entreprise : Nom commercial/Nom de l'entreprise, Code Budgétaire/Numéro du Registre de commerce, Nom du Directeur Général, Nom du Représentant Légal, Numéro de la CNI du Directeur Général ou du Représentant Légal, Nom de l'employé, Numéro de la CNI/Numéro de la carte de Résident/Séjour (Uniquement pour les étrangers) de l'employé, Nom du Mandataire, numéro de la CNI du Mandataire, période d'emploi, lettre donnant quitus au Mandataire pour faire la transaction au nom de l'entreprise, Informations sur l'utilisateur final du certificat (nom, numéro de la CNI, organisation, direction, téléphone (Bureau/Domicile/mobile), fax, e-mail) ;
- Informations sur l'impôt libérateur : Adresse et site des affaires, catégorie d'affaires, type d'affaires ;

- Individu : Nom, numéro de la CNI/Numéro de la carte de Résident/Séjour (uniquement pour les étrangers), e-mail, Téléphone (Bureau/Domicile/mobile).

② Informations optionnelles

- Individu: Adresse

**B. Sécurité des serveurs: le certificat SSL**

① Informations essentielles

- Organisme : Nom de l'Administration/Institution/Entreprise, Code Budgétaire/Numéro du Registre de Commerce, Nom du Président/Ministre/Recteur/Directeur Général, Nom de l'employé, Nom de l'administrateur du serveur, l'adresse de l'Administration/Institution/Entreprise

② Informations optionnelles

- Organisme : Informations sur l'administrateur du serveur (organisation, direction, Téléphone (Bureau/Domicile/mobile), fax, e-mail), Téléphone du Représentant Légal, adresse IP du serveur

**C. Enregistrement d'un nom de Domaine**

① Informations collectées lors de la souscription

- Informations essentielles : Nom, Numéro de la CNI/Numéro de la carte de Résident/Séjour (Uniquement pour les étrangers), Mot de passe, Nom de l'Administration/Institution/Entreprise, Code Budgétaire/Numéro du Registre de Commerce, Nom du Représentant Légal, Noms des techniciens (webmasters du site) adresse e-mail, Adresse, Téléphone (Bureau/Domicile/mobile), informations sur le représentant légal si celui-ci a moins de 12 ans, informations sur les serveurs DNS ;
- Informations Optionnelles: Fax, Nom/Adresse (pour sécuriser des informations essentielles sous la réglementation du nom de domaine);
- Moyens de paiement des informations à utiliser et des services : Il s'agit notamment de : Listing bancaires, détails de la carte de crédit.

② Informations collectées au moment de la souscription au service i-PIN

- Informations essentielles : Nom de l'Administration/Institution/ Entreprise, Nom du Représentant Légal, Nom de l'utilisateur réel du Certificat, Numéro de sa CNI/Numéro de sa carte de Résident/Séjour (uniquement pour les étrangers), Mot de passe, Code Budgétaire/Numéro du Registre de Commerce, Nom du Mandataire, Numéro de la CNI du Mandataire, adresse e-mail, Adresse, Téléphone (Bureau/Domicile/mobile), Informations sur le Représentant légal si celui-ci a moins de 12 ans (dans le cas d'une entreprise privée);
- Informations Optionnelles : Fax, Nom/Adresse (pour sécuriser les informations essentielles collectées lors de la souscription d'un nom de domaine selon la réglementation en vigueur);
- Moyens de paiement des informations à utiliser et des services. Il s'agit notamment de : Listing bancaires, détails sur la carte de crédit.

③ Les informations suivantes peuvent être créées et collectées dans le service utilisant le processus et traitant les Affaires commerciales

- Service utilisant le journal des événements, la connexion au journal des événements, cookie, informations sur la connexion par adresse IP, Listing de paiement, enregistrement des informations sur les délinquants économiques ;

- Organismes : Informations sur l'utilisateur réel du certificat de l'Administration/Institution Entreprise (Nom, numéro de la CNI, organisme, direction, Téléphone (Bureau/Domicile/mobile), fax, e-mail), Téléphone (Bureau/Domicile/mobile) du Représentant Légal.

#### **D. Clé du Service Mobile**

##### ① Informations essentielles

- Individu: Nom, Numéro de la CNI/Numéro de la carte de Résident/Séjour, Téléphone Mobile, Mot de passe d'accès à la clé Mobile, Nom de l'entreprise de service Mobile

##### ② Informations optionnelles

- Individu: e-mail

#### **E. Service de transaction avec les certificats**

##### ① Informations collectées au moment de la souscription

###### Informations essentielles

- Individu : Nom, Numéro de la CNI/Numéro de la carte de Résident/Séjour, Adresse, Nom d'utilisateur, Mot de passe, adresse e-mail
- Organisme : Nom de l'Administration/Institution/Entreprise, Nom commercial, Code budgétaire/Numéro du Registre de Commerce, Nom du Président/Ministre/Recteur/Directeur Général, Adresse, Nom du propriétaire du certificat, Mot de passe, Site de transactions et type de contenus, Téléphone (Bureau/Domicile/Mobile, fax), Informations sur l'utilisateur réel du certificat (nom, CNI, organisme, direction, Téléphone, adresse e-mail)

###### Informations optionnelles

- Individu: Téléphone Mobile
- Organismes : Informations sur l'utilisateur réel du certificat

##### ② Informations collectées au moment de la souscription au service i-PIN

###### Informations essentielles

- Individu: Nom de l'utilisateur, Adresse, Mot de passe, adresse e-mail

###### Informations optionnelles

- Individu: Téléphone Mobile

#### **F. Service de sauvegarde des documents électroniques**

① Informations essentielles: Nom, Numéro de la CNI/Numéro de la carte de Résident/Séjour (Uniquement pour les étrangers), Mot de passe, Informations sur le lieu de résidence, adresse e-mail, Adresse, Téléphone (Bureau/Domicile/mobile), question permettant une identification formelle du propriétaire des documents électroniques, Date et lieu d'émission du document électronique

② Informations optionnelles: Fax, encodage du certificat, nom du lieu de travail, direction, fonction, Téléphone (Bureau/Domicile/mobile), adresse du lieu de travail

#### **G. Contrat de Gestion du cycle de vie (CGC)**

① Informations essentielles: Nom de l'Institution/Administration/Entreprise, Code budgétaire/Numéro du Registre de Commerce, Nom du Président/Ministre/Recteur/Directeur Général, Numéro de la CNI/Numéro de la carte de Résident/Séjour de l'employé, Mot de passe, Téléphone (Bureau/Domicile/mobile) du Représentant Légal, adresse e-mail du Représentant Légal, Nom et genre de l'utilisateur réel du certificat, adresse e-mail

② Informations optionnelles: Fax, Date de naissance, Adresse, type d'affaires, catégorie d'affaires, adresse du site des affaires

## H. Service i-PIN de l'ANTIC

### Informations essentielles

- Individu: Nom de l'utilisateur du certificat, Numéro de la CNI/Numéro de la carte de Résident/Séjour, Mot de passe, adresse e-mail
- Organisme: Nom de l'Administration/Institution/Entreprise, Code budgétaire/Numéro du Registre de Commerce, Nom du Président/Ministre/Recteur/Directeur Général, Informations sur l'utilisateur réel du certificat (nom, CNI, fonction, Téléphone (Bureau/Domicile/Mobile), fax, e-mail)

### Informations optionnelles

- Individu: Téléphone Mobile
- Organismes: adresse du site, nom du site

### (2) Méthode de collecte des informations à caractère personnel

#### A. Service de certification ouvert au public

La page d'accueil contient le lien de téléchargement des demandes de certificats, la charte d'abonnement qui dit au demandeur à quoi il s'engage dans le service de certificat de l'ANTIC, l'autorité d'enregistrement de rattachement, etc.

#### B. Autres services

Services et produits qu'offre le système PKI aux utilisateurs, les méthodes de sécurisation des applications à l'aide de l'infrastructure à clé publique, etc.

## 2. L'objet de la procédure de collecte des informations confidentielles

L'ANTIC procède à la collecte des informations à caractère personnel dans les buts suivants :

### (1) Exécution du contrat et le règlement de charges

Prestation de service, acquisition et paiement de charges, diffusion de l'information nécessaire pour utiliser le service ou le produit, etc.

### (2) Gestion de la Clientèle

Vérification des informations à caractère personnel de l'utilisateur du certificat, identification de l'utilisateur du certificat, la prévention de l'utilisation des services de l'ANTIC par les utilisateurs de certificats délinquants, corrompus et la prévention de l'utilisation non autorisée, vérification de l'âge d'utilisation des services de l'ANTIC, traitement des affaires civiles telles que la plainte, la réponse aux sollicitations des clients et à la consultation, dépôt des notifications, service de traçabilité des activités illégales, etc.

### (3) Marketing et Publicité

Fourniture d'informations de la publicité pour un événement, etc... la publicité et la commercialisation du service de certificats ouvert au public et d'autres services offerts par l'ANTIC au public, la fréquence d'utilisation ou de connexion au service clientèle, des statistiques sur l'utilisation du service clientèle, etc.

## 3. Période de rétention des informations à caractère personnel

L'ANTIC procède et retient des informations à caractère personnel pour chaque service comme suit:

### (1) Service de certificats ouvert au Public

L'ANTIC sauvegarde et gère les informations et données des utilisateurs des certificats pour une période de 10 ans conformément aux dispositions prévues notamment par la Loi relative à cybersécurité et à la cybercriminalité, la Loi sur le commerce électronique. Dès lors, les informations recueillies ne peuvent être effacées de manière arbitraire, même sur la demande du client.

### (2) Autres services

L'ANTIC retient et utilise les informations à caractère personnel des utilisateurs de certificats dans le cadre d'autres services ouverts au public, uniquement pour la durée de ce service. Ces informations sont immédiatement détruites dès lors que la période d'utilisation est passée. En cas de non acceptation par le client de la collecte de ses informations à caractère personnel, celles-ci ne sont pas collectées et le service sollicité non fourni.

En cas de non continuité de service, l'ANTIC a le devoir de remettre lesdites informations aux autorités compétentes, notamment l'autorité de certification racine qui en assure la responsabilité, en attendant la mise en service d'une autre autorité de certification gouvernementale, etc.

Toutefois, les informations à caractère personnel sont conservées dans la confidentialité pendant une période de 10 ans, même lorsqu'elles sont requises pour besoins d'enquêtes, lors des règlements de litiges de service ou de procès, etc.

En outre, l'ANTIC sauvegarde les informations à caractère personnel des utilisateurs des certificats pour la période stipulée dans les Lois et Règlements du Cameroun, quand elles doivent être conservées selon la Loi régissant le Commerce électronique ou la Loi relative à la cybersécurité et à la cybercriminalité, etc.

A. Journal des comptes commerciaux et bordereaux de vente, 10 ans ? Documents importants, 5 ans ? Folio (Loi sur le Commerce électronique)

B. Livre des comptes, Documents de données probantes, 10/5 ans (Loi régissant le code des impôts, Loi sur les entreprises, Loi des impôts sur la Valeur Ajoutée, Code des marchés publics, etc)

C. Besoin de connexion en temps réel des communications passées pour la conservation des données de trafic, adresse IP, etc. 10 ans (Selon la loi régissant les communications électroniques, la loi sur le commerce électronique, la loi relative à la cybersécurité et à la cybercriminalité)

D. Enregistrement des informations indiquées: 6 mois (Loi sur la Protection des consommateurs, la loi régissant le commerce électronique, etc.)

E. Rétraction de l'enregistrement ou de la souscription de contrat : 10 ans (dispositions sur la protection du consommateur dans la loi régissant le commerce électronique, etc.)

F. Paiement et fourniture des biens enregistrés : 10 ans (Dispositions sur la protection des consommateurs dans la loi régissant le commerce électronique)

G. Plaintes de consommateurs et fiches de traitement des différends : 10 ans (Dispositions sur la protection des consommateurs dans la loi régissant le commerce électronique)

H. Collecte, traitement et utilisation des dossiers d'information sur le crédit : 10 ans (Dispositions sur l'utilisation et la protection de l'information sur le crédit du consommateur dans la loi régissant le commerce électronique)

#### **4. Fourniture des informations à caractère personnel à un tiers**

(1) L'ANTIC ne fournit ni ne révèle les informations à caractère personnel ou confidentielles des utilisateurs des certificats à un tiers sans leur consentement. Toutefois, lesdites informations peuvent être fournies sans leur consentement, conformément aux Lois et Règlements de la République, à la demande des institutions gouvernementales, Interpol, des Services de sécurité nationale et de défense, le Comité d'éthique de l'information et de la communication en cas de besoins d'enquêtes pour éclairer la justice sur des cas de

cybercriminalité, mais s'assure, après le traitement, que ces informations ne sont pas diffusées dans un cadre autre que celui pour lequel elles ont été sollicitées.

L'ANTIC peut mettre à la disposition des partenaires commerciaux ou des sociétés et coopératives des informations à caractère personnel des utilisateurs des certificats dans le but de leur fournir de meilleurs services, ceci dans le strict respect de la procédure de demande du consentement des concernés. Cela est possible après les avoir informés de l'objet, du contenu, de la raison, etc. Ces informations restent confidentielles lorsque l'utilisateur du certificat de l'ANTIC n'accorde pas son consentement.

En outre, elle passe par les procédures de demandes de consentement distinctes lorsque la fourniture des informations à caractère personnel dépasse la portée de son consentement préalable. Dans le cas où l'objet pour lequel ces informations ont été sollicitées est annulé, l'ANTIC demande à la Société les ayant demandées de les supprimer.

#### (2) Service de certification ouvert au public

L'ANTIC fournit des services de certification aux individus, ainsi qu'aux organisations du secteur public et du secteur privé en attendant que le secteur privé soit doté d'autorité(s) de certification accréditée(s). Le service de la clientèle de l'ANTIC sonde les utilisateurs des certificats en vue de rechercher leur satisfaction en optimisant le travail de consultation de la clientèle. Il peut être possible que l'utilisateur ne parvienne pas à régler sa facture du fait des erreurs portant sur les informations à caractère personnel contenues dans le certificat ou des inconvénients survenus lors de l'utilisation du service de consultation du certificat, ou lors du renouvellement du certificat ou de l'effet d'un événement ponctuel, dans ce cas le service de certification de l'ANTIC prendra toutes les mesures nécessaires pour ne pas exposer les informations à caractère personnel des utilisateurs de certificats aux cybercriminels.

Récepteurs	But	Fourniture d'informations	Période de rétention et d'utilisation
Service, Service de la Gestion clientèle de l'ANTIC	Le Service de la Gestion de la clientèle fonctionne comme un service de consultation des clients ou de télémarketing etc.	Tous les renseignements recueillis pour le service de certification	Termes de partenariat
KICA, GUCE	Suppression d'urgence lorsque la délivrance est illégale, par abus, etc. est rapporté	Nom, CNI/Numéro de la carte de résident, DN information, etc.	Suppression immédiate si pas client de l'ANTIC. Terminer la validité d'un certificat et sauvegarde pour 10 ans si client de l'ANTIC

#### (3) Service Mobile de Clé

L'ANTIC met à la disposition de ses clients la liste des services mobiles qu'elle fournit. Il s'agit notamment du Service de partenariat, du Service de la clientèle, du Service de marketing, ainsi que du service d'enregistrement des informations à caractère personnel des utilisateurs de certificats qui requièrent au préalable leur consentement. Les utilisateurs de certificats peuvent refuser la fourniture des informations confidentielles. Dans ce cas, le service mobile de clé ne peut leur être fourni.

Récepteurs	But	Information provision	Période de rétention et d'utilisation
Service clientèle de l'ANTIC mesurant la satisfaction des clients	Service clientèle fonctionnant comme consultation, etc.	Numéro Mobile, communication Mobile, nom de l'entreprise	Période d'utilisation du Service
Opérateurs de téléphonie Mobile (Camtel, MTN, Orange, Nexttel)	Vérification des propriétaires de téléphones mobiles	CNI/Numéro de la carte de séjour, Numéro Mobile	Période d'utilisation du Service

#### (4) Service de certificats ouvert au public

L'ANTIC publie sur son site la liste des informations à caractère personnel requises pour délivrer les certificats en vertu des Lois et Règlements en vigueur qui requièrent le consentement du

demandeur du certificat. Si le demandeur ne consent pas à mettre à la disposition des services de l'ANTIC ses informations à caractère personnel, il ne peut obtenir des services d'adhésion, tels que l'émission du certificat, son renouvellement, et tout autre service supplémentaire fourni par l'autorité de certification de l'ANTIC ou ses partenaires.

A. Noms des entreprises : ANTIC, KICA, Korea Internet & Security Agency (KISA), VeriSign, Comodo, Thawte, et Inicis

B. But : Fourniture des informations à caractère personnel lors de l'émission du certificat

C. Fourniture des Informations : Tous les renseignements fournis par le propriétaire et par la personne en charge de l'utilisation du certificat (Reportez-vous à la collecte des informations à caractère personnel)

D. Période de Rétention et d'utilisation

La période effective de rétention des informations à caractère personnel correspond à la durée réelle de l'utilisation du certificat par le contractant. Ces informations sont automatiquement supprimées dès la résiliation du contrat.

#### (5) Service d'enregistrement des noms de domaine

L'ANTIC publie la liste des informations à caractère personnel requises lors de l'enregistrement d'un nom de domaine (.cm) en conformité avec les lois et règlements de la République pour le consentement du client. Si un client ne consent pas, il ne peut pas recevoir la souscription à ce service et son nom de domaine ne peut être divulgué ni aucun autre service supplémentaire.

A. Nom de l'entreprise: ANTIC, Camtel, MTN, ICCSoft, Ringo, Creolink, Matrix, NetCom, InfoGenie, iServices, YooMe, WorldVoice, INET Consulting, Grid Engineering, FreeNom,

B. But: La fourniture des informations à caractère personnel lors de l'enregistrement des noms de domaine

C. Informations fournies: Tous les renseignements fournis par le propriétaire et la personne en charge de la gestion du nom de domaine

D. La période de Rétention et d'utilisation

Les informations à caractère personnel sont conservées pour la période d'utilisation effective du nom de domaine et automatiquement supprimées dès la résiliation du contrat.

#### (6) Service d'identification personnelle (IPIN)

L'ANTIC publie la liste des informations à caractère personnel demandées pour la fourniture du service d'identification personnelle en conformité avec les Lois et Règlements en la matière. Toutefois, le consentement du client est demandé. Si un client ne consent pas, son identification personnelle et d'autres informations à caractère personnel ne sont pas conservées sur des sites Web mettant en relief d'autres services d'identification personnelle, ainsi que des établissements d'identification personnelle.

1. Récepteurs des informations à caractère personnel

Service des informations à caractère personnel de l'ANTIC (CPKI), DGSN, DGRE, Interpol

2. But de l'utilisation des informations à caractère personnel par le récepteur des informations confidentielles

Cela permet une identification personnelle avec un i-PIN, indépendamment de l'institution d'identification personnelle, sur tous les sites utilisant les services d'identification personnelle.

3. Fourniture des informations à caractère personnel

Nom, groupe d'âge, genre, informations sur la nationalité, duplication des informations de prévention et de confirmation (DI)

4. Période de rétention et d'utilisation des informations à caractère personnel par le récepteur

Supprimées immédiatement après identification du client sur le site Web utilisé.

## **5. Organismes habilités à collecter des informations à caractère personnel**

### **(1) Service de certificats ouvert au public**

Pour fournir le service de certificats ouvert au public et améliorer l'accès de la clientèle et la convivialité, l'ANTIC signe un protocole d'accord avec chacun des organismes ayant sécurisé leurs applications à l'aide de la PKI nationale pour enregistrer les informations des demandeurs des certificats en les identifiant physiquement avant de procéder à la délivrance d'un certificat. Ces Administrations/entreprises gèrent pour le compte de l'ANTIC des autorités d'enregistrement. Elles collectent et gèrent des informations à caractère personnel des clients dans le strict respect des règles édictées par l'autorité de certification gouvernementale.

Les autorités d'enregistrement n'utilisent ou ne conservent les informations à caractère personnel des demandeurs de certificats pour d'autres fins que celles de l'émission du certificat, sauf si le client a expressément consenti aux dispositions autres que celles prévues par la loi.

## **6. Accès aux informations à caractère personnel**

### **(1) Service de certificats ouvert au public**

L'ANTIC fait tout son possible pour protéger les informations à caractère personnel des utilisateurs des certificats. L'Agence respecte strictement l'autorité de la personne pour les informations confidentielles, et leurs informations à caractère personnel peuvent être lues et corrigées à tout moment à partir du menu de la page d'accueil. Conformément à la loi relative à la cybersécurité et à la cybercriminalité, le certificat et les documents sur la cessation et la suppression des informations de l'utilisateur du certificat qui doivent être stockées en toute sécurité pendant 10 ans à compter de la date d'expiration du certificat.

### **(2) Autres services**

L'ANTIC fait tout son possible pour protéger les informations à caractère personnel des utilisateurs des certificats. L'Agence respecte strictement l'autorité de la personne pour les informations confidentielles, et leurs informations à caractère personnel peuvent être lues et corrigées à tout moment à partir du menu de la page d'accueil. L'utilisateur de certificat peut se rétracter et retirer son consentement à l'utilisation du certificat à tout moment, lorsque l'adhésion est annulée.

## **7. Suppression des informations à caractère personnel**

### **(1) Service de certificats ouvert au public**

L'ANTIC supprime immédiatement les informations à caractère personnel de l'utilisateur du certificat à la fin des 10 ans de la période de rétention légale. La procédure de suppression et la méthode d'effacement sont les suivantes:

- A. Procédure de suppression : Les documents présentés par le client en vue de l'utilisation du service sollicité sont supprimés après avoir été retenus pendant 10 ans à compter de la date d'expiration du certificat, en vertu des dispositions de la loi relative à la cybersécurité et à la cybercriminalité, ainsi que la Loi régissant le commerce électronique.
- B. Méthode de destruction: Les documents et les demandes de certificats stockés dans un espace physique sont détruits à l'aide d'une déchiqueteuse, ou calcinés par une personne habilitée dans une zone contrôlée. Les informations à caractère personnel stockées sur

support électronique sont supprimées à l'aide d'une méthode technique qui rend impossible la restauration des dossiers des clients.

(2) Autres services

L'ANTIC supprime immédiatement les informations à caractère personnel lorsque l'objet pour lequel elles ont été recueillies a pris fin selon la loi. La procédure et la méthode de suppression sont les suivantes.

A. Procédure de suppression

Les informations fournies par le client lors de la souscription d'adhésion au Service de certificats sont déplacées de la base de données (DB) lorsque l'objet pour lequel elles ont été collectées n'est plus valable. Dans ce cas, elles sont supprimées après avoir été stockées pendant une certaine période (voir période de rétention et d'utilisation) conformément à la réglementation en vigueur au Cameroun sur la protection des informations à caractère personnel. Les informations ainsi déplacées de la DB ne sont pas utilisées à d'autres fins que celles pour lesquelles elles sont requises.

B. Méthode de suppression

Les informations à caractère personnel enregistrées dans un fichier électronique sont supprimées en utilisant une technique qui rend impossible la restauration du dossier.

## **8. Mesures protectives des informations à caractère personnel**

(1) Service de certificats/Service Mobile de clé

L'ANTIC utilise un (système de mise en quarantaine) de pare-feu pour bloquer le vol, la fuite, la falsification, la déformation des renseignements personnels par craquage (piratage malveillant) etc. Le pare-feu est installé sur chaque serveur et dans le réseau pour suivre les invasions/intrusions illégales. L'ANTIC effectue également la sauvegarde régulière des informations à caractère personnel du demandeur de certificat pour prévenir les accidents possibles.

(2) Autres services

L'ANTIC fait tout son possible pour prendre les mesures techniques et administratives afin d'empêcher la fuite des informations à caractère personnel des utilisateurs des certificats à des fins criminelles. L'utilisateur de certificat peut accéder à ses informations à caractère personnel en utilisant son mot de passe et peut les modifier en utilisant son certificat. Par conséquent, le client doit veiller à ce que ce mot de passe ne soit pas révélé à d'autres personnes.

L'utilisateur est responsable de la sécurité de sa clé privée et du mot de passe associé. Par conséquent, l'ANTIC ne prend aucune responsabilité sur l'émission du certificat de l'utilisateur dans une machine utilisée par le public, notamment dans un cybercafé, dans un télécentre communautaire.

Pour protéger la clé privée et le mot de passe associé, lors de l'utilisation du certificat dans les espaces publics, comme un cybercafé, un accès public à l'Internet ou lors du partage de l'ordinateur avec d'autres personnes, une attention particulière pour éviter la divulgation des informations à caractère personnel doit être mise lors de la déconnexion après avoir utilisé le service.

En outre, pour créer un mot de passe, il convient de combiner des chiffres, des lettres et des caractères spéciaux. Il est souhaitable de changer de mot de passe fréquemment pour prévenir les fuites accidentelles.

En outre, l'ANTIC minimise les risques et contrôle le personnel manipulant des informations à caractère personnel, et prend des mesures correctives immédiatement quand un problème se pose.

## **9. Le demandeur de Certificat ou le représentant légal**

Le demandeur de certificat ou le représentant légal (pour les enfants de moins de 12 ans ou pour les plus âgés) peuvent se renseigner et corriger les informations à caractère personnel de l'utilisateur de certificat ou demander l'annulation du service.

Les demandes en vue de la correction des informations à caractère personnel peuvent être effectuées en utilisant le menu "corriger les informations de l'utilisateur". Lorsque vous contactez l'opérateur en charge de la gestion des informations à caractère personnel pour annuler le service (par lettre ou par e-mail), la demande est immédiatement exécutée après traitement de la procédure d'identification personnelle.

## **10. Amendement de la Politique de confidentialité**

Le contenu de la politique de confidentialité peut être lu à n'importe quel moment sur la page d'accueil du site web de l'autorité de certification gouvernementale et les amendements se font suivant la réglementation en vigueur, pour un meilleur service. Visitez donc régulièrement la page d'accueil de la CamGovCA pour voir le contenu.

Lorsque le contenu de la politique de confidentialité est amendé, l'ANTIC la publie sur la page d'accueil de chaque service.

## **11. Personne en charge de la gestion des informations à caractère personnel**

Les demandes de renseignements sur les informations à caractère personnel sont envoyées aux points de contacts suivants et l'ANTIC vous répondra aussi rapidement que possible.

Personne en charge de la protection des informations à caractère personnel

Nom : ESSIANE ELLA Justin

Direction : Centre d'Infrastructure Nationale à Clé Publique

Téléphone : +237 242 08 64 97

Adresse: B. P. 6170, Yaoundé-Cameroun.

Sites web : [www.antic.cm](http://www.antic.cm) [www.camgovca.cm](http://www.camgovca.cm) [www.rootca.cm](http://www.rootca.cm);

e-mail: [pki@antic.cm](mailto:pki@antic.cm)

Numéro de téléphone des Services de renseignements à contacter

- Centre d'appels : +237 242 08 64 97
- Service de certificats : +237 242 08 64 97
- Service de certificats SSL : +237 242 08 64 97
- Service d'enregistrement des noms de domaine : +237 242 09 91 64
- Service de la veille sécuritaire : +237 242 09 91 64
- Service d'horodatage : +237 242 08 64 97
- Service de Statut de certificat en temps réel : +237 242 08 64 97
- Service Public de sauvegarde des documents électroniques : +237 242 08 64 97
- Service de Gestion des contrats : +237 242 08 64 97

## **12. Notification obligatoire**

Lorsque le contenu de la politique de confidentialité est modifié, l'ANTIC informe sa clientèle sur sa page d'accueil au moins 7 jours avant l'exécution de l'amendement.

- Date de notification : 06 Juillet 2015
- Date de prise d'effet : 13 Juillet 2015