Remarque :

Le présent document est les conditions générales d'utilisations, ci-après appelée CGU, de TN PKI CA de l'Agence nationale de certification Electronique en Tunisie (dénommée ANCE). Ce document ne remplace pas la politique de certification ni la déclaration des pratiques de certification (PC / DPC) en vertu de laquelle les certificats Electronique de l'ANCE sont émis. Cette déclaration, qui suit la structure de l'annexe A du document ETSI TS 411 319-1, Est simplement informative et ne remplace en aucun cas les dispositions des documents

1. Informations et Contacts :

Les requêtes concernant cette déclaration de divulgation d'ICP doivent être adressées à: L'Agence Nationale de Certification Electronique,

Adresse: Technopark El Ghazala, Route de Raoued Km 3.5, Ariana 2083 - Tunisie

E-mail: ndca.pki@certification.tn

Tél: +216 70 834 600

Fax: +216 70 834 555

Site web: www.certification.tn

2. OBJET

Les présentes Conditions Générales d'Utilisation ont pour objet de préciser le contenu et les modalités d'utilisation des CERTIFICATS VPN (OID [GOV] 2.16.788.1.2.6.1.9.1.6 ; OID [CORP] 2.16.788.1.2.6.1.9.2.6), Signature de code et signature de code EV (OID [GOV] 2.16.788.1.2.6.1.9.1.4 ; OID [CORP] 2.16.788.1.6.1.9.2.4) proposés par l'ANCE ainsi que les engagements et obligations respectifs des différents acteurs concernés.

3. DEFINITIONS

CLIENT : Organisme, personne morale, professionnel qui contracte avec l'ANCE pour disposer de CERTIFICATS.

CERTIFICAT VPN : désigne un certificat ayant pour objet d'associer des informations relatives à certains nœuds du réseau (routeurs, firewalls, concentrateurs …) à une clé publique. Ce certificat est utilisé pour garantir la sécurité des échanges effectués entre une organisation et ses filiales à travers des tunnels sécurisés dans le réseau de communication.

CERTIFICATS DE SIGNATURE DE CODE : désigne un certificat électronique ayant pour objet de signer un programme, un script ou un logiciel pour garantir son authenticité par la signature de son développeur. Il permet aussi de le protéger contre le risque de piratage.

CONTRAT : Ensemble contractuel constitué des présentes Conditions Générales d'Utilisation, du formulaire de demande de CERTIFICAT ainsi que les procédures figurant sur le site www.certification.tn applicables à la date de conclusion du CONTRAT.

MANDATAIRE : Personne physique ayant directement, par la loi, par délégation ou par procuration du CLIENT, le pouvoir d'accomplir tout acte nécessaire à la demande d'émission et à la conclusion et à l'exécution du CONTRAT ainsi que des obligations relatives à la gestion de tout CERTIFICAT portant le nom du CLIENT, qui aura été émis à la demande et sous la responsabilité de ladite personne. A défaut de désignation express, le MANDATAIRE est un Représentant légal du CLIENT. Le MANDATAIRE est responsable des agissements des LE PORTEUR OU LE MANDATAIRE .

LE PORTEUR: désigne la personne physique identifiée dans le Certificat et qui est le détenteur de la Clé Privée correspondant à la Clé Publique qui est dans ce Certificat.

LISTE DE CERTIFICATS REVOQUES (« LCR ») : liste horodatée et régulièrement mise à jour des Certificats Électroniques Révoqués, créée et Signée Électroniquement par l'AC ayant émis les Certificats Électroniques.

Révocation : désigne l'action qui a pour but l'extinction de la validité du Certificat. Un Certificat qui a fait l'objet d'une Révocation est inscrit sur la LCR.

« Conditions Générales » ou « CGU » : désigne les présentes conditions générales d'utilisation.

Extented Validation ou EV : désigne le type de certificat avec validation approfondie.

Organisation Validation : Désigne le type de certificat avec validation de l'organisation

DPC : Déclaration des pratiques de certification

PC : Politique de Certification.

OCSP est un protocole Internet permettant de vérifier la validité d'un certificat numérique TLS en temps-réel auprès de l'autorité ayant émis le certificat.

4. Type de certificat, procédures de validation et utilisation :

Cette déclaration ne s'applique qu'aux services de certification qualifiés fournis par l'ANCE. Les certificats qualifiés de clé publique sont délivrés par l'autorité de certification qualifiée «TnTrust Gov CA» ou « TnTrust Corporate CA » . Le profil et toute autre limitation du certificat de clé publique certifié délivré par le «TnTrust Gov CA» ou « TnTrust Corporate CA » sont conformes à l'ETSI EN 319 411-2.

Procédure de validation :

Le certificat qualifié est délivré à un particulier après vérification de son identité. La vérification de la personne peut être effectuée par une autorité d'enregistrement ou toute autre personne autorisée à confirmer l'identité du titulaire du certificat. La personne qui demande la délivrance d'un certificat qualifié doit être identifiée par sa pièce d'identité nationale. Dans le cas d'individus associés ou agissant pour le compte d'une organisation, l'autorisation de l'abonné (le signataire) d'agir et d'utiliser le certificat pour le compte de l'organisation est requise ou l'enregistrement officiel des pouvoirs est exigé du gouvernement ou du registre du commerce.

L'identification et l'authentification du demandeur d'un certificat doivent répondre aux exigences précisées à la section 3.2 (Validation initiale de l'identité) du PC / DCP. L'Autorité de Certification ou l'Autorité d'enregistrement doit identifier et authentifier toutes les informations d'abonné requises en vertu de la section 3.2 (Validation initiale de l'identité) du PC / DPC susmentionné.

Usage

Les certificats qualifiés délivrés par «TnTrust Gov CA» ou « TnTrust Corporate CA » ne peuvent être utilisés que conformément à EN ETSI TS 319 411-2.

Limite de service :

Certificat VPN : n'est utilisé que pour l'authentification d'un Tunnel VPN seulement

Certificat de signature de code OV et EV : n'est utilisé que pour la signature de code seulement

5. UTILISATEUR DE CERTIFICAT :

Désigne une personne qui fait confiance aux CERTIFICATS DE SIGNATURE DE CODE, afin d'identifier et signer son programme ou script, ou aux CERTIFICATS VPN , afin de identifier et sécuriser les informations échangées

Le Client s'engage à n'utiliser les Certificats qui lui sont délivrés qu'en son nom propre. Ainsi, il lui est interdit d'utiliser le Certificat pour le compte d'autres organisations.

6. DUREE

Le CONTRAT est conclu à compter de la réception du dossier du CLIENT par l'ANCE.

Le CONTRAT est conclu pour une durée correspondant à la durée de vie du CERTIFICAT.

L'attestation établie par le CLIENT conformément à l'article 7, manifeste son consentement de poursuivre sa relation contractuelle avec l'ANCE aux Conditions Générales d'Utilisation applicables au moment du renouvellement du CERTIFICAT.

7. PRIX

Sauf accord express préalable intervenu avec l'ANCE, le prix mentionné dans l'offre commerciale est payable à la commande.

Le CLIENT s'engage, lors du dépôt du dossier d'inscription, à payer le prix mentionné suivant les modalités convenues.

Le CLIENT accepte que l'ANCE encaisse le prix convenu dès réception de son dossier d'inscription complet. En cas de dossier d'inscription incomplet, le CLIENT est informé immédiatement et le dossier n'est pas pris en compte. Si la demande a été effectuée via le site web de l'ANCE, le client dispose de deux jours ouvrables pour fournir les pièces manquantes sans quoi la demande est rejetée sans retenue financière.

Dans le cas d'une demande via le site web de l'ANCE, l'Agence transmettra au CLIENT une facture lors de la livraison du CERTIFICAT. Dans le cas d'une demande via un guichet, la facture est émise dès le paiement des frais de certificat.

En cas de renouvellement du CERTIFICAT, une nouvelle demande doit être faite conformément à l'article 7 et les frais sont de nouveau à la charge du CLIENT sauf erreur de l'ANCE dans les informations du CERTIFICAT. Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat.

8 . VALIDITE DE L'OFFRE – PRISE D'EFFET DU CONTRAT

Les CGU sont opposables au CLIENT dès leur signature et, à défaut de signature, dès la première utilisation du Certificat qui implique l'acceptation pleine et entière des CGU par le CLIENT.

Les CGU sont conclues et opposables pendant toute la durée de vie du Certificat.

L'ANCE s'engage à répondre à toute demande du CLIENT répondant aux Conditions Générales d'Utilisation mises en ligne sur www.certification.tn. En tout état de cause, l'ANCE se réserve la faculté de refuser le traitement de toute demande soumise aux Conditions Générales d'Utilisation qui ne sont plus disponibles sur le site www.certification.tn.

9. Limites de confiance

L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » ne fixent pas de limite de fiabilité pour les certificats délivrés en vertu de cette politique. La limite de confiance peut être fixée par d'autres politiques, contrôles applicatifs et loi applicable en Tunisie ou par l'accord de la partie qui fait confiance.

Afin de gérer le fonctionnement du système ANCE et de superviser les utilisateurs et le personnel de l'ANCE tous les événements se produisant dans le système et ayant un impact essentiel sur la sécurité de l'ANCE et tous les événements liés au cycle de vie des clés gérées par l'Autorité de Certification, y compris toutes les paires de clés objet générées par l'Autorité de Certification sont enregistrés.

10. ENGAGEMENTS DE L'ANCE

L'ANCE est expressément tenue à une obligation de moyen pour toutes les obligations relatives à la gestion du cycle de vie du CERTIFICAT qu'elle émet.

En cas de rejet de la demande, l'ANCE en informe le PORTEUR OU LE MANDATAIRE en spécifiant la raison du rejet ainsi que la liste des champs incorrects ou incomplets.

Dans le cas d'une demande via un guichet, le client est informé immédiatement des pièces manquantes à fournir sans relance et le dossier n'est pas pris en compte.

L'ANCE s'engage à informer le client des spécifications techniques nécessaires à la génération de sa requête lors de sa demande de certificat soit directement soit par mail, soit par Téléphone.

Les informations de révocation des certificats sont disponibles sur le serveur OSCP à l'adresse http://va.certification.tn.

L'ANCE met à la disposition de ses PORTEUR OU LE MANDATAIRE un service technique en ligne consistant en une liste de question (« FAQ ») et une messagerie électronique. Le support technique est quant à lui joignable au 70835555 ou par mail à assistance@certification.tn.

L'ANCE déclare et garantit qu'aucune erreur n'a été introduite par l'ANCE dans les informations du Certificat du fait d'un manque de soin de l'ANCE lors de la création du Certificat ;
Que son émission de Certificats est totalement conforme à sa déclaration CPS (Certification Practice Statement) ;
Et que ses services de révocation et son utilisation d'un Référentiel sont totalement conformes à sa déclaration CPS.
Note : le certificat de signature de code EV est livré sur un support cryptographique sécurisé.

11. ENGAGEMENTS DU CLIENT

Le Porteur ou LE MANDATAIRE est tenu d'agir conformément au PC / DPC et à la convention d'abonné pertinente. Dans ce contexte, Le Porteur ou LE MANDATAIRE est responsable de:

• Avoir une compréhension de base de la bonne utilisation de la cryptographie à clé publique et des certificats;

• Ne fournir que des informations correctes sans erreurs, omissions ou fausses déclarations;

• Fournir des renseignements probants en fournissant un formulaire d'inscription dûment rempli et signé

• Compléter ces informations par une preuve d'identité et la fourniture des informations;

• Vérifier le contenu d'un certificat nouvellement délivré avant sa première utilisation et s'abstenir si elle contient des renseignements trompeurs ou inexacts.

• Lire et accepter tous les termes et conditions de ce PC / DPC et autres Règlements et accords;

• Assurer le contrôle total de la clé privée en ne partageant pas les clés privées et / ou Les mots de passe;

• Notifier à l'autorité d'enregistrement de tout changement apporté à l'un des renseignements contenus dans le certificat ou tout changement de circonstances qui rendrait les renseignements du certificat trompeurs ou inexacts;

• Invalider immédiatement le certificat si les informations contenues dans le certificat sont trompeuses ou inexactes ou, en cas de changement de circonstances, rendant le certificat trompeur ou inexact;

• Notifier immédiatement à l'autorité d'enregistrement de tout soupçon ou toute compromis de la clé privée et demandant la révocation du certificat;

• Cesser immédiatement d'utiliser le certificat

L'expiration ou la révocation d'un tel certificat

Tout dommage ou corruption présumée ou réelle de la clé privée correspondant à la clé publique dans un tel certificat, et enlever immédiatement le certificat des dispositifs et / ou logiciels sur lesquels il a été installé;

• S'abstenir d'utiliser la clé privée de PORTEUR ou de MANDATAIRE correspondant à la clé publique du certificat pour signer d'autres certificats;

• Protéger la clé privée des accès non autorisés.

Les Informations permettant à l'autorité d'enregistrement de contacter le PORTEUR OU LE MANDATAIRE (numéro de téléphone, courriel, etc.). Au minimum, une adresse de courrier électronique doit être sous de la forme « admin », « administrator », «webmaster », « hostmaster », ou « postmaster »@ le nom du domaine demandé dans le certificat et que ce dernier lui appartient.

LE PORTEUR OU LE MANDATAIRE, a été (depuis sa création) et restera l'unique détenteur de sa clé privée, de son code PIN et de tout dispositif logiciel ou matériel protégeant sa clé privée, et qu'aucune personne non autorisée n'a eu ou n'aura accès à ces éléments.

Toute modification d'information signalée comme obligatoire lors de l'enregistrement ou du renouvellement du CERTIFICAT doit être notifiée par écrit à l'ANCE et accompagnée des justificatifs requis.

En outre, toute modification affectant le statut du CLIENT doit être notifiée immédiatement à l'ANCE (notamment, redressement judiciaire, dissolution, liquidation).

Le PORTEUR OU LE MANDATAIRE s'engage à vérifier l'exactitude de son certificat ainsi que de l'accepter et autoriser sa publication

12. Obligations de vérification des statuts de certificats des parties fiables

Les parties prenantes ne sont autorisées à utiliser les certificats que conformément aux conditions énoncées dans le PC / DCP. Il est de leur seule responsabilité de vérifier la validité juridique et les politiques applicables.

Pour vérifier la validité d'un certificat électronique qu'ils ont reçu, les parties fiables doivent se référer à la réponse LCR ou OCSP avant de s'appuyer sur l'information présentée dans un certificat pour s'assurer que l'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » CA n'a pas révoqué le certificat. Les emplacements du point de distribution LCR et du répondant OCSP sont détaillés dans le certificat. Une partie de confiance est engagée à:

• Effectuer des opérations cryptographiques de manière précise et correcte en utilisant le logiciel et les dispositifs dont le niveau de sécurité est conforme au niveau de sensibilité du certificat en cours de traitement et le niveau de confiance des certificats appliqués,

13. ENGAGEMENTS DES UTILISATEURS DE CERTIFICATS

Les Utilisateurs de Certificats s'engagent à respecter les stipulations des CGU.

Les Utilisateurs de Certificats vérifient et respectent l'usage pour lequel un Certificat a été émis.

Les Utilisateurs de Certificats contrôlent que le Certificat émis par l'ANCE est référencé au niveau de sécurité et pour le service de confiance requis par l'application.

Les Utilisateurs de Certificats peuvent vérifier les LCR (Listes des certificats révoqués) sur http://www.certification.tn/tntrustcorporateca.crl, http://www.certification.tn/tntrustqualifiedcorporateca.crl http://www.certification.tn/tntrustqualifiedgovca.crl , http://www.certification.tn/tntrustgovca.crl, http://crl.certification.tn.

La LCR est publiée et accessible au public sur des serveurs disponibles 24/7

REVOCATION DU CERTIFICAT

- Un Certificat sera révoqué pour les causes suivantes:

- modification d'une information contenue dans le Certificat ;

- Informations inexactes fournies dans le dossier d'enregistrement ;

- Compromission possible ou avérée de la Clé Privée du PORTEUR ou DU MANDATAIRE ;

- Non-respect par le PORTEUR ou LE MANDATAIRE des règles d'utilisation du Certificat ;

- Non-respect par le PORTEUR ou LE MANDATAIRE ou le Client de la PC/DPC de l'ANCE ;

- Réalisations d'opérations frauduleuses ;

- Résiliation de l'abonnement ;

- Demande de révocation du Certificat par le Client;

- Cessation de l'activité du PORTEUR ou DU MANDATAIRE au sein du Client et ce, quelle qu'en soit la cause : décès, démission... ;

- Dysfonctionnement du support physique ou de son logiciel pilote associé ;

- Vol ou perte du support physique du Certificat ;

- Cessation d'activité du Client.

Une demande de révocation du Certificat pourra être faite à tout moment par fax ou en ligne à partir du site Internet suivant: http:// eservices.ance.tn.

La demande de révocation peut émaner des personnes suivantes :

- Le MANDATAIRE du Client;

- Le PORTEUR ou LE MANDATAIRE ;

En cas de vol ou de perte du support physique et lorsque plusieurs Certificats sont stockés sur ce même support, la demande de révocation du PORTEUR ou LE MANDATAIRE devra porter sur l'ensemble de ces Certificats.

La demande de révocation fait l'objet d'une procédure de vérification des informations relatives au demandeur et de son autorité par rapport au Certificat. Le PORTEUR ou LE MANDATAIRE reçoit une confirmation par e-mail de cette révocation.

Le PORTEUR ou LE MANDATAIRE reconnaît et accepte qu'il supportera l'entière responsabilité de toute utilisation du Certificat après avoir eu connaissance de la survenance d'un des événements susmentionnés, sans préjudice de toute action en responsabilité que l'ANCE se réserve le droit d'exercer contre le Le PORTEUR ou LE MANDATAIRE .

L'ANCE : En cas d'erreur (intentionnelle ou non) détectée dans le dossier ou dans le processus d'enregistrement du Le PORTEUR ou LE MANDATAIRE .

Le certificat dont la révocation a été demandée à l'ANCE est placé sans délai dans la liste de certificats révoqués (LCR). La LCR est publiée et accessible au public sur des serveurs disponibles 24/7

https://www.certification.tn/crl_mail.crl, https://www.certification.tn/crl_web.crl , http://crl.certification.tn.

DEBLOCAGE DU CERTIFICAT: Le PORTEUR OU LE MANDATAIRE est le seul responsable du blocage de son code PUK (cela après trois tentatives erronées).

14. ETENDUE DE RESPONSABILITE

14.1 Limites de responsabilité

• Fournir des services de délivrance et de dépôt de certificats en conformité avec le PC / DCP et les autres politiques et procédures d'exploitation de l'ANCE

Au moment de l'émission du certificat, «TnTrust Gov CA» ou « TnTrust Corporate CA » met en œuvre la procédure pour vérifier l'exactitude des informations qui y sont contenues avant l'installation et la première utilisation,

• Mettre en œuvre une procédure visant à réduire la probabilité que les informations du certificat n'est pas trompeur,

• Maintenir 24 x 7 dépôts accessibles au public avec des informations actuelles,

• Effectuer les procédures d'authentification et d'identification conformément au PC / DPC et aux politiques et procédures internes d'exploitation,

• Fournir des services de gestion de certificats et de clés, y compris l'émission de certificats, la publication et la révocation conformément à la «TnTrust Gov CA» ou « TnTrust Corporate CA » PC / DPC,

• Le PORTEUR ou LE MANDATAIRE ou les parties prenantes ne faisant aucune garantie ou promesse directe.

L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » n'est pas responsable de la perte du service PKI:

-En raison de guerre, de catastrophes naturelles, etc.

-En raison de l'utilisation non autorisée de certificats ou de l'utilisation de celle-ci au-delà de l'utilisation prescrite définie par la «TnTrust Gov CA» ou « TnTrust Corporate CA » PC / DPC admissible pour les certificats délivrés par l'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA »

14.2 Exonération de responsabilité

• L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » n'assumera aucune responsabilité le PORTEUR ou LE MANDATAIRE ou toute autre personne dans la mesure où cette responsabilité résulte de leur négligence, de leur fraude ou de leur mauvaise conduite délibérée.

• L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » n'assume aucune responsabilité quant à l'utilisation des Certificats ou des paires de Clés Publiques / Clés Privées associées émises en vertu de la Politique de Certification pour toute utilisation autre que conformément à la Politique de Certification. Les souscripteurs indemniseront L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » de toute responsabilité et coûts ainsi que les réclamations qui en découlent.

• L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » ne sera pas responsable de toute partie quiconque pour tout dommage subi directement ou indirectement à la suite d'une perturbation incontrôlable de ses services.

• Les Utilisateurs finaux sont tenus responsables de toute forme de fausse déclaration des informations contenues dans le certificat à des parties fiables même si les informations ont été acceptées par L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA »

• Les Clients pour compenser une Partie qui fait confiance qui encourt une perte en raison de la violation par le PORTEUR ou LE MANDATAIRE de l'accord du Client.

L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » nie toute responsabilité financière ou de toute autre nature pour les dommages ou les dépréciations découlant de son exploitation de l'autorité de certification.

15. RESILIATION

Au cas où l'une des parties n'exécuterait pas l'une des obligations découlant des présentes Conditions Générales d'Utilisation, l'autre partie lui notifiera d'exécuter ladite obligation.

A défaut pour la partie défaillante d'avoir exécuté dans les trente jours de cette notification, l'autre partie pourra résilier le CONTRAT sans préjudice des dommages-intérêts.

En cas de résiliation anticipée, quel qu'en soit le motif du CONTRAT conclu entre l'ANCE et le CLIENT, les sommes acquittées lors de la souscription du CONTRAT restent acquises par l'ANCE pour toute prestation commencée.

16. NOTIFICATION ET CONVENTION DE PREUVE

Dans le cadre des échanges entre les parties, la date de réception du message par le destinataire et la signature de ce message valent preuves entre elles et justifient que la notification est imputable à la partie émettrice du dite message.

17. DONNEES A CARACTERE PERSONNEL

L'ANCE respecte pleinement la loi tunisienne sur la protection des données à caractère personnel et toute autre loi applicable en Tunisie.

Toute information sur les abonnés qui n'est pas rendue publique à travers les certificats émis par L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » ou la LCR est considéré comme une information privée. Toute information rendue publique dans un certificat délivré par L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » , ou de sa LCR, ou par un service accessible au public ne doit pas être considérée comme confidentielle.

L'ANCE conserve tous les événements relatifs au cycle de vie des clés gérées par l'autorité de certification pendant au moins 20 ans après que tout certificat basé sur ces enregistrements cesse d'être valide.

18. Ententes applicables, DPC et PC

La PC/ DPC du L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » peut être trouvée sur le site Web de l'ANCE à http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf.

Pour ce qui est de l'accord d'abonnement et de l'accord sur la partie qui fait confiance, ils peuvent être consultés sur le site Web de l'ANCE à http://www.certification.tn

19. Politique de remboursement

À l'heure actuelle, L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » ne prélève pas de frais pour les certificats numériques, bien que L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » se réserve le droit de le modifier à l'avenir. Certificats numériques pour lesquels aucun frais n'est facturé, aucun remboursement n'est possible. En outre, un Fournisseur de services de certifications gouvernemental ou un Fournisseurs de services de certifications d'entreprise peut facturer des frais pour son service

20. INTEGRALITE DU CONTRAT

Les parties prenantes reconnaissent que les présentes Conditions Générales d'Utilisation, et toutes les procédures figurant sur le site www.certification.tn constituent l'intégralité des accords entre elles en ce qui concerne la réalisation de l'objet des présentes, et annulent et remplacent tous accords et propositions antérieurs ayant le même objet quelle qu'en soit la forme.

21. CESSION DU CONTRAT

Le CONTRAT est réputé avoir été conclu en considération de la personne du CLIENT. C'est pourquoi le CLIENT s'interdit de céder le contrat sans l'accord exprès et préalable de l'ANCE qui n'a pas à fournir de justification de sa décision.

22. INDEPENDANCE DES PARTIES

D'une façon générale, chacune des parties est une personne physique ou morale indépendante juridiquement et financièrement, agissant en son nom propre et sous sa seule responsabilité.

23. LOI APPLICABLE

Les certificats délivrés par L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » , le PC/ DPC, le Contrat d'Abonné sont régis par les lois et règlements de la Tunisie.

En cas de litige ou de controverse entre les parties, y compris les partenaires de l'ANCE, le PORTEUR ou LE MANDATAIRE et les Parties Confédérales, seront soumis à la juridiction des tribunaux de district d'Ariana en Tunisie.

24. Licences CA et Repository, marques de confiance et audit

Une vérification annuelle est effectuée par un vérificateur externe indépendant afin d'évaluer la conformité de L'autorité de certification «TnTrust Gov CA» ou « TnTrust Corporate CA » aux normes CA WebTrust / ETSI.

Il est possible de procéder à plus d'un audit de conformité par an si cela est demandé par la partie vérifiée ou s'il résulte de résultats insatisfaisants d'une vérification antérieure.

Les audits de conformité des CA nationaux tunisiens sont effectués par un cabinet d'expertise comptable qui:

• Démontre la maîtrise de l'ETSI pour les autorités de certification,

• Démontre la maîtrise de la technologie d'infrastructure à clé publique, des outils et des techniques de sécurité de l'information, de l'audit de sécurité et de la fonction d'attestation de tiers,

• Certifié, accrédité, autorisé ou autrement évalué comme répondant à la qualification

Exigences des vérificateurs dans le cadre du système d'audit,

• Est lié par la loi, la réglementation gouvernementale ou le code de déontologie professionnelle.

LA SIGNATURE DU FORMULAIRE DE DEMANDE DE CERTIFICAT MANIFESTE LA PRISE DE CONNAISSANCE ET L'ADHESION DU CLIENT AUX PRESENTES CONDITIONS GENERALES D'UTILISATION ET AUX PROCEDURES FIGURANT SUR LE SITE WWW.CERTIFICATION.TN, AINSI QUE SON CONSENTEMENT POUR L'UTILISATION DE CES DONNEES A CARACTERE PERSONNELLE POUR LA GENERATION DU CERTIFICAT DEMANDEUR