IMPORTANT

Veuillez lire attentivement le présent Contrat d'Abonné avant de demander, d'accepter ou d'utiliser un Certificat SSL de TunTrust.

Le présent Contrat est conclu entre la personne physique ou morale identifiée sur le ou les Certificats émis résultant du présent Contrat (« Abonné du Certificat ») et l'Agence Nationale de Certification Electronique - TunTrust. Le présent Contrat régit la demande et l'utilisation par l'Abonné d'un Certificat SSL émis par TunTrust. L'utilisation d'un Certificat implique l'acceptation de ce Certificat.

TunTrust et l'Abonné conviennent de ce qui suit :

1. DÉFINITIONS

- **Abonné** : Personne physique ou morale à qui un Certificat est délivré et qui est juridiquement liée par un Contrat d'abonnement.
- **Adresse IP** : un numéro de 32 bits ou 128 bits attribué à un périphérique qui utilise le protocole Internet pour la communication.
- **Autorité de Certification (AC)** : Organisation responsable de la création, de l'émission, de la révocation et de la gestion du cycle de vie des Certificats.
- **Autorité d'Enregistrement (AE)** : désigne une entité approuvée par l'AC, afin d'enregistrer les demandes d'émission, de renouvellement et de révocation de Certificats, de les valider ou de les rejeter.
- **Baseline Requirements** : Les « Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates » telles que publiées par le « CA/Browser Forum » et tout amendement à ce document.
- **Bureau d'enregistrement de noms de domaine** : une personne ou une entité qui enregistre des noms de domaine sous les auspices de ou en accord avec : (i) l'Internet Corporation for Assigned Names and Numbers (ICANN), (ii) une autorité/un registre national des noms de domaine, ou (iii) un centre d'information du réseau *Network Information Center* (y compris leurs affiliés, sous-traitants, délégués, successeurs ou cessionnaires).
- **Certificat** : Un document électronique qui utilise une signature numérique pour lier une clé publique à une identité.
- **Certificat de nom de domaine générique (*Wildcard*)** : un Certificat contenant au moins un nom de domaine générique dans le champ « Autre nom de l'objet » (*Subject Alternative Names*) contenu dans le Certificat.
- **Certificat Valide** : un Certificat qui réussit la procédure de validation spécifiée dans la RFC 5280.
- **Clé Compromise** : une clé privée est dite compromise si sa valeur a été divulguée à une personne non autorisée ou si une personne non autorisée y a eu accès.
- **Clé privée** : La clé d'une paire de clés qui est gardée secrète par le détenteur de la paire de clés et qui est utilisée pour créer des signatures numériques.
- **Clé publique** : la clé d'une paire de clés qui peut être divulguée publiquement par le détenteur de la clé privée correspondante et qui est utilisée par une partie utilisatrice pour vérifier les signatures numériques créées avec la clé privée correspondante du détenteur et/ou pour chiffrer les messages afin qu'ils ne puissent être déchiffrés qu'avec la clé privée correspondante du titulaire.
- **Contrat d'Abonné** : Le présent accord entre l'AC et le demandeur/Abonné qui précise les droits et les responsabilités des parties, disponible sur https://www.tuntrust.tn/repository .
- **Date d'expiration** : La date "Valide jusqu'a" dans un Certificat définit la fin de la période de validité d'un Certificat.
- **Déclarations des Pratiques de Certification (DPC)** : l'un des nombreux documents formant le cadre de gouvernance dans lequel les Certificats sont créés, délivrés, gérés et utilisés.
- **Demandeur** : La personne physique qui demande (ou demande le renouvellement) d'un Certificat. Une fois le Certificat émis, le Demandeur est désigné comme Abonné.
- **Entité légale** : une association, une société, un partenariat, une entreprise individuelle, une fiducie, une entité gouvernementale ou une autre entité ayant un statut juridique dans le système juridique d'un pays.
- **Label de domaine** : de la RFC 8499 (http://tools.ietf.org/html/rfc8499) : "Une liste ordonnée de zéro ou plusieurs octets qui constitue une partie d'un nom de domaine. En utilisant la théorie des graphes, un label identifie un nœud dans une partie du graphique de tous les noms de domaine possibles."
- **Liste de Révocation de Certificats (CRL)** : Une liste des Certificats révoqués régulièrement mise à jour qui est créée et signée numériquement par l'AC qui a émis les Certificats.
- **Nom de domaine** : Une liste ordonnée d'un ou plusieurs labels de domaine attribuées à un nœud dans le système de noms de domaine.

- **Nom de Domaine Entièrement Qualifié *(FQDN)***: Un nom de domaine qui inclut les labels de domaine de tous les nœuds supérieurs du système de noms de domaine Internet.
- **Nom de domaine enregistré** : un nom de domaine qui a été enregistré auprès d'un bureau d'enregistrement de noms de domaine.
- **Nom de domaine générique (*Wildcard*)** : une chaîne commençant par "*." (U+002A ASTÉRISQUE, U+002E POINT) immédiatement suivi d'un Nom de Domaine Entièrement Qualifié.
- **Paire de Clés** : La Clé Privée et sa Clé Publique associée.
- **Partie utilisatrice** : toute personne physique ou entité juridique qui s'appuie sur un Certificat Valide. Un Fournisseur de Logiciels d'Application n'est pas considéré comme une Partie utilisatrice lorsque le logiciel distribué par ce Fournisseur affiche simplement des informations relatives à un Certificat. Les parties utilisatrices doivent lire et accepter l'accord de partie utilisatrice de TunTrust disponible sur https://www.tuntrust.tn/repository.
- **Période de Validité** : La période de validité est telle que définie dans la RFC 5280, section 4.1.2.5 : la période de temps du champs « Valide à partir du » (*notBefore*), à « Valide jusqu'a» (*notAfter*), inclus.
- **Politique de Certification (CP)** : désigne l'ensemble de règles publiées par l'AC, décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE et des utilisateurs des Certificats. La version applicable de la Politique de Certification de TunTrust est disponible dans le lien suivant : https://www.tuntrust.tn/repository, et inclut les versions successives mises à jour publiées sur ce site.
- **Protocole d'état de Certificat en ligne (OCSP)** : protocole de vérification de Certificat en ligne qui permet au logiciel d'application de la partie utilisatrice de déterminer l'état d'un Certificat identifié.
- **Répondeur OCSP** : Un serveur en ligne exploité sous l'autorité de l'AC pour le traitement des demandes d'état de Certificat.
- **Repository** : une base de données en ligne contenant des documents de gouvernance de la PKI rendus publics (tels que des politiques de Certification et des déclarations de pratiques de Certification) et des informations sur l'état des Certificats, sous la forme d'une CRL ou d'une réponse OCSP.
- **Titulaire de nom de domaine** : parfois appelé le « propriétaire » d'un nom de domaine, mais plus exactement la ou les personnes ou entités enregistrées auprès d'un bureau d'enregistrement de nom de domaine comme ayant le droit de contrôler la manière dont un nom de domaine est utilisé, comme la personne physique ou l'entité juridique répertoriée comme « Titulaire » par WHOIS ou le bureau d'enregistrement du nom de domaine.

2. FRAIS

Les frais d'inscription et d'émission d'un Certificat SSL sont disponibles pour le public sur le site web de TunTrust https://www.tuntrust.tn/ .

Lors de la soumission par le Demandeur d'une demande dûment remplie d'un Certificat SSL et de l'acceptation de cette demande par TunTrust, l'Abonné doit payer tous les frais applicables pour le Certificat avant l'émission du Certificat demandé.

Après l'émission du Certificat, aucun autre frais ne sera appliqué pour l'utilisation des Certificats SSL.

Tous les paiements sont non remboursables.

3. UTILISATION, OBJET ET LIMITATIONS

Les Certificats OV SSL de TunTrust sont utilisés pour sécuriser les communications et les transactions en ligne. Le Certificat OV SSL permet à l'entité finale de prouver son identité aux autres participants et de maintenir l'intégrité de la transaction.

Le Certificat SSL est valable pendant toute la Période de Validité indiquée dans le Certificat, sauf révocation antérieure. Le présent Contrat reste en vigueur pendant toute la période pendant laquelle le Certificat est Valide et prendra fin à l'expiration ou à la révocation du Certificat de l'Abonné.

4. ROLE ET OBLIGATIONS DE L'ABONNE

Avant d'accepter et d'utiliser un Certificat OV SSL de TunTrust, l'Abonné doit : (i) générer sa propre Paire de Clés ; (ii) soumettre une demande pour un Certificat OV SSL de TunTrust ; et (iii) accepter et consentir aux termes du présent Contrat d'Abonné. L'Abonné est seul responsable de la protection de la Clé Privée sous-jacente au Certificat de TunTrust.

L'Abonné s'assure de:

a) L'exactitude des informations : fournir à tout moment des informations exactes et complètes à TunTrust lors de la demande de Certificat ;
b) La protection de la Clé Privée : prendre toutes les mesures raisonnables pour assurer le contrôle, garder confidentielle et protéger correctement à tout moment la Clé Privée qui correspond à la Clé Publique à inclure dans le(s) Certificat(s) demandé(s) (et toute donnée ou dispositif d'activation associé, par exemple mot de passe ou jeton) ;
c) L'acceptation du Certificat : examiner et vérifier l'exactitude du contenu du Certificat ;
d) L'utilisation du Certificat : installer le Certificat uniquement sur les serveurs accessibles au(x) « Autre nom de l'objet » répertorié(s) dans le Certificat et utiliser le Certificat uniquement en conformité avec toutes les lois applicables et uniquement conformément au présent Contrat d'Abonné;
e) L'alerte et la révocation : pour : (i) demander rapidement la révocation du Certificat et cesser de l'utiliser, ainsi que sa Clé Privée associée, en cas d'utilisation abusive ou de compromission réelle ou présumée de la Clé Privée de l'Abonné associée à la Clé Publique incluse dans le Certificat, et (ii) demander rapidement la révocation du Certificat et cesser de l'utiliser, si des informations contenues dans le Certificat sont ou deviennent incorrectes ou inexactes ;
f) La résiliation de l'utilisation du Certificat : cesser rapidement toute utilisation de la Clé Privée correspondant à la Clé Publique incluse dans le Certificat lors de la révocation de ce Certificat pour des raisons de Clé Compromise ;
g) La réactivité : pour répondre aux instructions de TunTrust concernant la Clé Compromise ou l'utilisation abusive du Certificat dans un délai spécifié ;
h) La reconnaissance et l'acceptation : avoir reconnu et accepté que TunTrust a le droit de révoquer le Certificat immédiatement si l'Abonné devait violer les termes du présent Contrat ou si la révocation est requise par la PC/DPC de TunTrust PKI ou les Baseline Requirements du CA/B Forum.

5. REVOCATION

TunTrust révoque un Certificat dans les 24 heures si un ou plusieurs des événements suivants se produisent :

a) L'Abonné demande par écrit à TunTrust de révoquer le Certificat à travers l'outil de révocation en ligne https://www.tuntrust.tn/Revocation-online-service ou en se présentant physiquement devant un opérateur de l'AE de TunTrust ;
b) TunTrust obtient la preuve tangible que la demande de Certificat d'origine n'était pas autorisée et n'accorde pas d'autorisation rétroactivement ;
c) TunTrust obtient la preuve que la Clé Privée de l'Abonné correspondant à la Clé Publique figurant dans le Certificat a subi une compromission
d) TunTrust est informée d'une méthode démontrée ou prouvée qui peut facilement calculer la Clé Privée de l'Abonné en fonction de la Clé Publique du Certificat (telle qu'une clé Debian faible, voir https://wiki.debian.org/SSLkeys) ; ou
e) TunTrust obtient la preuve que la validation de l'autorisation ou du contrôle de domaine pour tout Nom de Domaine Entièrement Qualifié ou adresse IP dans le certificat ne serait pas fiable.

TunTrust révoque un Certificat dans les 05 jours si un ou plusieurs des événements suivants se produisent :

a) Le Certificat n'est plus conforme aux exigences des sections 6.1.5 et 6.1.6 de la PC/DPC « TunTrust PKI CP/CPS » concernant les Paires de Clés ;
b) TunTrust obtient la preuve que le Certificat a été mal utilisé ;
c) TunTrust est informé que l'Abonné a violé une ou plusieurs de ses obligations matérielles en vertu du Contrat d'Abonné ;
d) TunTrust est mise au courant de toute circonstance indiquant que l'utilisation d'un Nom de Domaine Entièrement Qualifié ou d'une adresse IP dans le Certificat n'est plus légalement autorisée (par exemple, un tribunal ou un arbitre a révoqué le droit d'un Titulaire d'un Nom de Domaine d'utiliser le Nom de Domaine, un accord de licence ou de services pertinent entre le Titulaire du Nom de Domaine et le Demandeur a pris fin, ou le Titulaire du Nom de Domaine n'a pas renouvelé le Nom de Domaine) ;
e) TunTrust est mise au courant qu'un Certificat de nom de domaine générique a été utilisé pour authentifier un Nom de Domaine Entièrement Qualifié subordonné frauduleusement trompeur ;
f) TunTrust est mise au courant d'un changement important dans les informations contenues dans le Certificat ;

g) TunTrust est mise au courant que le Certificat n'a pas été émis conformément aux Baseline Requirements ou à la PC/DPC « TunTrust PKI CP/CPS »;
h) TunTrust détermine ou est mise au courant que l'une des informations figurant dans le Certificat est inexacte ;
i) Le droit de TunTrust d'émettre des Certificats en vertu des Baseline Requirements du CA/B Forum expire ou est révoqué ou résilié, à moins que TunTrust n'ait pris des dispositions pour continuer à maintenir le Repository de la LCR/OCSP ;
j) La révocation est exigée par la PC/DPC « TunTrust PKI CP/CPS »; ou
k) TunTrust est mise au courant d'une méthode démontrée ou prouvée qui expose la Clé Privée de l'Abonné à un compromis, ou s'il existe des preuves claires que la méthode spécifique utilisée pour générer la Clé Privée était défectueuse.

Un Certificat peut être révoqué pour l'une des raisons suivantes. Si la situation est que plusieurs raisons de révocation s'appliquent, la raison de révocation la plus prioritaire (selon l'ordre de la liste suivante) doit être indiquée :

a) Compromission de clé (RFC 5280 CRLReason #1): L'Abonné doit choisir la raison de révocation " Compromission de clé " lorsqu'il a des raisons de croire que la Clé Privée de son Certificat a été compromise, par exemple, une personne non autorisée a eu accès à la Clé Privée de son Certificat.
b) Cessation d'opération (RFC 5280 CRLReason #5): L'Abonné devrait choisir la raison de révocation " Cessation d'opération" lorsqu'il ne possède plus tous les Noms de Domaine du Certificat ou lorsqu'il n'utilisera plus le Certificat parce qu'il interrompt son site web.
c) Changement d'affiliation (RFC 5280 CRLReason #3): L'Abonné devrait choisir la raison de révocation "Changement d'affiliation" lorsque le nom de leur organisation ou d'autres informations organisationnelles dans le Certificat ont changé.
d) Remplacé (RFC 5280 CRLReason #4): L'Abonné devrait choisir la raison de révocation "Remplacé" lorsqu'il veut demander un nouveau Certificat pour remplacer le Certificat existant.
e) Non-spécifié (RFC 5280 CRLReason #0): Lorsque les raisons de révocation ci-dessus ne s'appliquent pas à la demande de révocation, l'Abonné ne doit pas fournir de raison autre que "Non-spécifié".

6. EXCLUSION DE GARANTIE

Dans la mesure permise par la loi en vigueur, le Contrat d'Abonné et tout autre document contractuel applicable, TunTrust ne fait aucune représentation ou garantie expresse ou implicite en vertu de la PC/DPC "TunTrust PKI CP/CPS". TunTrust décline expressément toute garantie expresse ou implicite de quelque nature que ce soit à quiconque, y compris toute garantie implicite de titre, de non-contrefaçon, de qualité marchande ou d'adéquation à un usage particulier.

7. LIMITATION DE RESPONSABILITE ET DOMMAGES

TunTrust n'est responsable que des dommages résultant de son non-respect de la PC/DPC "TunTrust PKI CP/CPS" et provoqués délibérément ou par négligence.

TunTrust n'est en aucun cas responsable des pertes de bénéfices, des dommages indirects et consécutifs, ou de la perte de données, dans la mesure permise par la loi Tunisienne. TunTrust n'est pas responsable des dommages résultant des violations par l'Abonné ou les parties utilisatrices de Certificats des conditions générales applicables.

TunTrust n'est en aucun cas responsable des dommages résultant de forces majeures telles que décrits dans la PC / DPC "TunTrust PKI CP/CPS". TunTrust prend des mesures commercialement raisonnables pour atténuer les effets de la force majeure en temps voulu. Les dommages résultant de tout retard causé par la force majeure ne seront pas couverts par TunTrust.

L'Abonné est responsable vis-à-vis de TunTrust et des parties utilisatrices de Certificats de tout dommage résultant d'une mauvaise utilisation, d'une faute intentionnelle, du non-respect des obligations réglementaires ou du non-respect d'autres dispositions relatives à l'utilisation du Certificat**.**

8. PROTECTION DES DONNEES A CARACTERE PERSONNEL

TunTrust respecte pleinement la loi Tunisienne sur la protection des données à caractère personnel et toute autre loi applicable en Tunisie.

Toute information d'Abonné qui n'est pas rendue publique par le biais de Certificats émis par TunTrust est considérée comme une information privée. Toute information rendue publique dans un Certificat émis par TunTrust ou par un service accessible au public fourni par TunTrust ne sera pas considérée comme confidentielle.
TunTrust conserve tous les événements du cycle de vie des Certificats pendant au moins 20 ans après la fin de la validité de tout Certificat basé sur ces enregistrements**.**

9. INDEMNISATION

Dans la mesure permise par la loi en vigueur, chaque Abonné doit libérer, indemniser et dégager de toute responsabilité l'AC de TunTrust, ainsi que tous les administrateurs, actionnaires, dirigeants, agents, employés, sous-traitants et successeurs de TunTrust de ce qui précède, contre toute perte, dommage ou dépense, y compris les honoraires d'avocat, liés à (i) toute fausse déclaration ou omission de la part de l'Abonné, que la fausse déclaration ou l'omission soit intentionnelle ou non ; (ii) la violation par l'Abonné de son Contrat d'Abonné, de la PC/DPC "TunTrust PKI CP/CPS" ou de la loi applicable ; (iii) la compromission ou l'utilisation non autorisée d'un Certificat ou d'une Clé Privée causée par la négligence ou des actes intentionnels de l'Abonné ; ou (iv) l'utilisation abusive par l'Abonné d'un Certificat ou d'une Clé Privée.

10. AMENDEMENTS

TunTrust peut modifier le présent Contrat, les PC/DPC de TunTrust, son site web et tout document répertorié sous son Repository (https://www.tuntrust.tn/repository) à tout moment en publiant soit l'amendement, soit le document modifié dans son site web. L'Abonné doit consulter périodiquement le Repository pour être au courant de tout changement. L'Abonné peut résilier le présent Contrat s'il n'accepte pas la modification apportée. L'utilisation continue du Certificat par l'Abonné après la publication d'une modification constitue l'acceptation de la modification par l'Abonné.

11. TRANSPARENCE DES CERTIFICAT

Pour s'assurer que les Certificats fonctionnent correctement tout au long de leur cycle de vie, TunTrust peut enregistrer les Certificats SSL avec une base de données publique de transparence des Certificats. Étant donné que cela deviendra une exigence pour la fonctionnalité du Certificat, l'Abonné ne peut pas se retirer de ce processus. Les informations du serveur de journalisation sont accessibles au public. Une fois soumises, les informations ne peuvent pas être supprimées d'un serveur de journalisation.

12. AVIS

L'Abonné adressera toutes les notifications à TunTrust par courrier écrit avec accusé de réception, à :

Agence Nationale de Certification Electronique,
Adresse :Parc Technologique El Ghazala, Route de Raoued km 3.5, Ariana, 2083, Tunisie.

Vous consentez qu'en demandant, en acceptant ou en utilisant un Certificat SSL TunTrust, vous reconnaissez avoir lu le présent Contrat, que vous le comprenez et que vous en acceptez les termes. Si vous demandez, acceptez ou utilisez un Certificat SSL au nom d'une entreprise ou d'une autre Entité Légale, vous déclarez que vous êtes un représentant autorisé de cette entité et que vous avez le pouvoir d'accepter ce Contrat au nom de cette entité. Si vous ne disposez pas d'une telle autorité ou si vous n'acceptez pas le présent Contrat, ne demandez pas, n'acceptez pas et n'utilisez pas un Certificat SSL de TunTrust.

NOM, PRENOM ET SIGNATURE