

IMPORTANT

Veillez lire attentivement les présentes Conditions Générales d'Utilisation avant de demander, d'accepter ou d'utiliser un Certificat ID-Trust ou DigiGo de TunTrust.

Le présent Contrat est conclu entre la personne physique 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 ID-Trust ou DigiGo émis par TunTrust. L'utilisation d'un Certificat implique l'acceptation de ce Certificat.

TunTrust et l'Abonné conviennent de ce qui suit :

1. DEFINITIONS

- **Abonné** : Personne physique ou morale à qui un Certificat est délivré et qui est juridiquement liée par un Contrat d'abonnement.
- **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.
- **Autorité d'Enregistrement Centrale (AEC)**: TunTrust exploite une Autorité d'Enregistrement Centrale (AEC) qui enregistre les Abonnés des Certificats émis par les AC de TunTrust. L'AEC interagit indirectement par l'intermédiaire des AEDs et/ou directement avec les Abonnés et directement avec l'AC pour fournir des services de certification.
- **Autorité d'Enregistrement Déléguée (AED)**: TunTrust délègue l'exécution de ses fonctions à des Autorités d'Enregistrement Déléguées qui doivent respecter toutes les exigences de la convention AED et la PC/DPC applicable. Les AED ont pour objet d'opérer un ou plusieurs PVP et VVS et procèdent, dans des conditions strictement déterminées et contrôlées, à la validation de l'identité du Demandeur.
- **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.
- **Certificat**: Un fichier électronique qui utilise une signature numérique pour lier une clé publique à une identité.
- **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'au" 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.
- **Défectueux** : Un support cryptographique est considéré défectueux par TunTrust s'il présente les aspects suivants :
 - Le support ne peut pas correctement stocker ou protéger les clés cryptographiques conformément aux spécifications techniques dans la PC/DPC correspondante.
 - Le support cryptographique ne peut plus être accédé ou utilisé avec les dispositifs ou logiciels compatibles, malgré des tentatives de réinitialisation de mot de passe ou de déblocage moyennant les dispositifs mis à disposition par TunTrust.
- **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.
- **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.
- **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.
- **Point de Vérification Physique:** Un Point de Vérification Physique dépend toujours d'une AED. La mission principale des Points de Vérification Physique (PVP) est de (i) collecter les données personnelles du Demandeur, y compris le nom complet, la date et le lieu de naissance, l'adresse e-mail, le numéro de téléphone portable ; (ii) fournir la preuve de la présence physique du Demandeur et (iii) remettre la documentation à l'AED où toutes les demandes de Certificat sont recueillies et transmises en toute sécurité à l'AEC.
- **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.
- **Service de Vérification Vidéo (VVS):** Un service de vérification vidéo peut être fourni par une AED afin d'authentifier à distance l'identité physique d'une personne. La mission principale d'un Service de Vérification Vidéo est de (i) collecter les données personnelles du Demandeur, y compris le nom complet, la date et le lieu de naissance, l'adresse e-mail, le numéro de téléphone portable ; (ii) faire une copie numérique du document d'identification du demandeur (passeport, carte d'identité ou titre de séjour) et (iii) confirmer les données personnelles du Demandeur dans une vidéo en direct pour compléter les documents d'identification et visant à éviter la fraude à l'identification.

2. FRAIS

Les frais d'inscription, d'émission et d'utilisation d'un Certificat ID-Trust ou DigiGo sont disponibles pour le public sur le site web de TunTrust.

Lors de la soumission par le Demandeur d'une demande dûment remplie d'un Certificat ID-Trust ou DigiGo, 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 les Certificats ID-Trust, toutefois, pour les Certificats DigiGo, d'autres frais d'utilisation du Certificat sont applicables.

Tous les paiements sont non remboursables.

3. UTILISATION, OBJET ET LIMITATIONS

Les Certificats ID-Trust et DigiGo sont utilisés pour authentifier l'Abonné auprès d'une variété de services gouvernementaux en ligne et pour signer des documents électroniques. Le Certificat est valable pendant toute la Période de Validité indiquée dans le Certificat, sauf révocation antérieure. Le présent Contrat reste en vigueur pendant toute la durée de validité du Certificat et prendra fin à l'expiration ou à la révocation du Certificat de l'Abonné.

4. ROLE ET OBLIGATIONS DE L'ABONNE

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 donnée d'activation de la Clé Privée (code PIN) ;
- c) L'acceptation du Certificat : examiner et vérifier l'exactitude du contenu du Certificat ;
- d) L'utilisation du Certificat : utiliser le Certificat uniquement en conformité avec toutes les lois applicables et uniquement conformément au présent Contrat ;
- 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 inexacts ;
- 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 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.

5. REVOCATION

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

1. L'Abonné demande de révoquer son Certificat ID-Trust à travers l'outil de révocation en ligne de TunTrust disponible sur <https://www.tuntrust.tn/Revocation-online-service> ;
2. L'Abonné demande de révoquer son Certificat DigiGo en accédant à son espace privé au niveau de <https://digigo.tuntrust.tn> ou à travers le lien <https://digigo.tuntrust.tn/pub/revoke> ;
3. L'Abonné demande de révoquer son Certificat ID-Trust en accédant à son espace privé au niveau de <https://ecert.tuntrust.tn> ;
4. L'Abonné demande par écrit à TunTrust de révoquer le Certificat en se présentant physiquement devant un opérateur de l'AE de TunTrust ;
5. TunTrust obtient la preuve tangible que la demande de Certificat d'origine n'était pas autorisée et n'accorde pas d'autorisation rétroactivement ou bien que l'Abonné ne soit plus en capacité d'utiliser son Certificat (dans le cas d'un décès, etc.) (CRLReason #9, privilegeWithdrawn);
6. TunTrust obtient une demande de révocation de la part des AED (si applicable) ;
7. TunTrust obtient la preuve que la Clé Privée de l'Abonné correspondant à la Clé Publique figurant dans le Certificat a subi une compromission ou n'est plus conforme aux exigences de la PC/DPC applicable (CRLReason #1, keyCompromise);
8. 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>) (CRLReason #1, keyCompromise) ; ou
9. TunTrust obtient la preuve que la validation de l'adresse e-mail contenue dans le Certificat ne serait pas fiable (CRLReason #4, superseded).

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

1. Le Certificat n'est plus conforme aux exigences des sections 6.1.5 et 6.1.6 de la PC/DPC applicable concernant les Paires de Clés (CRLReason #4, superseded);
2. TunTrust obtient la preuve que le Certificat a été mal utilisé (CRLReason #9, privilegeWithdrawn);
3. TunTrust est informé que l'Abonné a violé une ou plusieurs de ses obligations matérielles en vertu du Contrat d'Abonné (CRLReason #9, privilegeWithdrawn);
4. TunTrust est informé de toute circonstance indiquant que l'utilisation d'une adresse électronique dans le certificat n'est plus légalement autorisée (par exemple, un tribunal ou un arbitre a révoqué le droit d'utiliser une adresse électronique, un accord de licence ou de services pertinent entre l'abonné a pris fin, ou le titulaire du compte n'a pas réussi à maintenir le statut actif de l'adresse électronique) (CRLReason #5, cessationOfOperation) ;

5. TunTrust est mise au courant d'un changement important dans les informations contenues dans le Certificat (CRLReason #9, privilegeWithdrawn);
6. TunTrust est mise au courant que le Certificat n'a pas été émis conformément aux Baseline Requirements ou à la PC/DPC applicable (CRLReason #4, superseded);
7. TunTrust détermine ou est mise au courant que l'une des informations figurant dans le Certificat est inexacte (CRLReason #9, privilegeWithdrawn);
8. 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 CRL/OCSP (CRLReason "unspecified (0)");
9. La révocation est exigée par la PC/DPC applicable pour un motif qui n'a pas été spécifié dans la présente section (CRLReason "unspecified (0)"); ou
10. 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 (CRLReason #1, keyCompromise).

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 n'utilisera plus le Certificat.
- 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 demande un nouveau Certificat pour remplacer son 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 applicable. 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, sauf pour le cas des certificats ID-Trust comme suit : Si l'Abonné constate, dans un délai de 45 jours suivant la date d'expédition de son Certificat, que son support cryptographique est Défectueux, il est en droit de demander à TunTrust un remplacement sans frais supplémentaires.

7. LIMITATION DE RESPONSABILITE ET DOMMAGES

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

TunTrust n'est en aucun cas responsable des pertes de bénéficiaires, 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 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 applicable 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. 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 ID-Trust ou DigiGo 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 ID-Trust ou DigiGo 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 ID-Trust ou DigiGo de TunTrust.

NOM, PRENOM ET SIGNATURE