

Formulaire d'Adhésion en Qualité d'Entité Déléguée (pour l'Enregistrement des Demandes de Certificat) et/ou d'Intégrateur de Signature Électronique à Distance				N° Dossier (A remplir par TunTrust)	
Informations sur l'entité					
Identifiant Unique					
Raison Sociale					
Adresse de l'entité					
N°, Rue, App					
Code postal		Ville			
Gouvernorat		Pays			
Informations sur le représentant légal					
Nom et Prénom					
N°Pièce d'identité		<input type="radio"/> CIN	<input type="radio"/> Passeport	<input type="radio"/> Carte de séjour	
Tél. professionnel					
Email professionnel					
Informations sur l'interlocuteur unique					
Nom et Prénom					
N°Pièce d'identité		<input type="radio"/> CIN	<input type="radio"/> Passeport	<input type="radio"/> Carte de séjour	
Fonction					
Tél. professionnel		Mobile			
Email professionnel					
Liste des Services Proposés					
Enregistrement des demandes de certificat DIGIGO PRO PERSO SEAL		<input type="radio"/> Oui <input type="checkbox"/> Identification Vidéo <input type="checkbox"/> Identification Face-à-face		<input type="radio"/> Non	
Services de signature électronique à distance		<input type="radio"/> Oui <input type="checkbox"/> Signature au nom de l'entité morale <input type="checkbox"/> Signature au nom de la personne physique		<input type="radio"/> Non	

1 Délégation du Service d'Enregistrement des Demandes de Certificats Digigo

TunTrust s'appuie sur un réseau d'entité d'enregistrement constitué d'une Autorité d'Enregistrement Centrale (AEC) opérée par TunTrust et un ensemble d'Entités Déléguées d'enregistrement (ED) ayant conclu un accord contractuel avec TunTrust, indiquant l'autorisation de leur rôle en tant qu'ED et précisant clairement leurs obligations et leurs responsabilités conformément à la PC/DPC de TunTrust.

L'Autorité d'Enregistrement Centrale de TunTrust est responsable des fonctions suivantes :

- Identifier et authentifier les demandeurs de certificats,
- Accepter, évaluer, approuver ou rejeter l'enregistrement des demandes de certificat,
- Demander l'émission d'un certificat via un processus d'authentification multi-facteurs suite à l'approbation d'une demande de certificat,
- Authentifier et traiter les demandes de révocation de certificats,
- Archiver les fichiers d'enregistrement (électroniques et / ou papier),
- Assurer l'assistance technique aux porteurs de certificats.

L'AEC de TunTrust peut déléguer l'opération de la vérification des identités des demandeurs (authenticité des pièces d'identité présentées, comparaison de caractéristiques physiques du demandeur, etc.) à une Entité Déléguée qui accepte de s'acquitter de ses fonctions en vertu de l'accord contractuel conformément à la Loi 83-2000 du 9 août 2000, relative aux échanges et au commerce électronique et la PC/DPC de TunTrust en vigueur et disponible sur le site web <https://www.tuntrust.tn/repository>.

1.1 Vérification de l'identité du demandeur

Dans le cadre d'un accord contractuel, TunTrust peut déléguer le service de vérification de l'identité du demandeur à une entité déléguée. Cette dernière est tenue d'établir une identification rigoureuse des demandeurs de certificat notamment à travers la vérification d'une pièce d'identité avec photo (CIN, Passeport, Carte de Séjour). L'ED doit également vérifier l'identité d'une personne morale à travers l'extrait du Registre National des Entreprises et éventuellement la carte d'identification fiscale.

La vérification de l'identité d'un individu peut se faire soit par identification physique (face-à-face) soit par identification vidéo et ce comme suit :

- La vérification de l'identité du demandeur peut se faire lors d'un entretien en face-à-face avec le demandeur à condition que l'ED soit :
 - - Un établissement public ou privé soumis à une législation ou une réglementation relative à l'identification du client « KYC » dans le cadre de leur activité.
 - - Un établissement public offrant des services aux citoyens à travers des guichets centraux et régionaux exigeant la présence physique du citoyen pour son identification.
- La vérification de l'identité du demandeur peut se faire par identification vidéo selon une procédure d'enregistrement approuvée par TunTrust conformément aux exigences détaillées dans l'accord contractuel .

L'ED doit indiquer dans le formulaire d'adhésion la méthode de vérification d'identité qui sera mise en œuvre pour l'enregistrement des demandes de certificat.

1.2 Les opérateurs de vérification

Les opérateurs chargés des services de vérification de l'identité du demandeur de certificat doivent être employés de l'entité déléguée.

L'ED doit fournir la liste complète des opérateurs de vérification conformément au formulaire fourni ci-dessous. Tout changement des opérateurs doit être signalé immédiatement à TunTrust.

L'ED doit utiliser une application d'enregistrement des demandes de certificat audité par TunTrust. L'application d'enregistrement peut être mobile ou web. Tout changement fonctionnel apporté à l'application d'enregistrement audité doit être signalé à TunTrust.

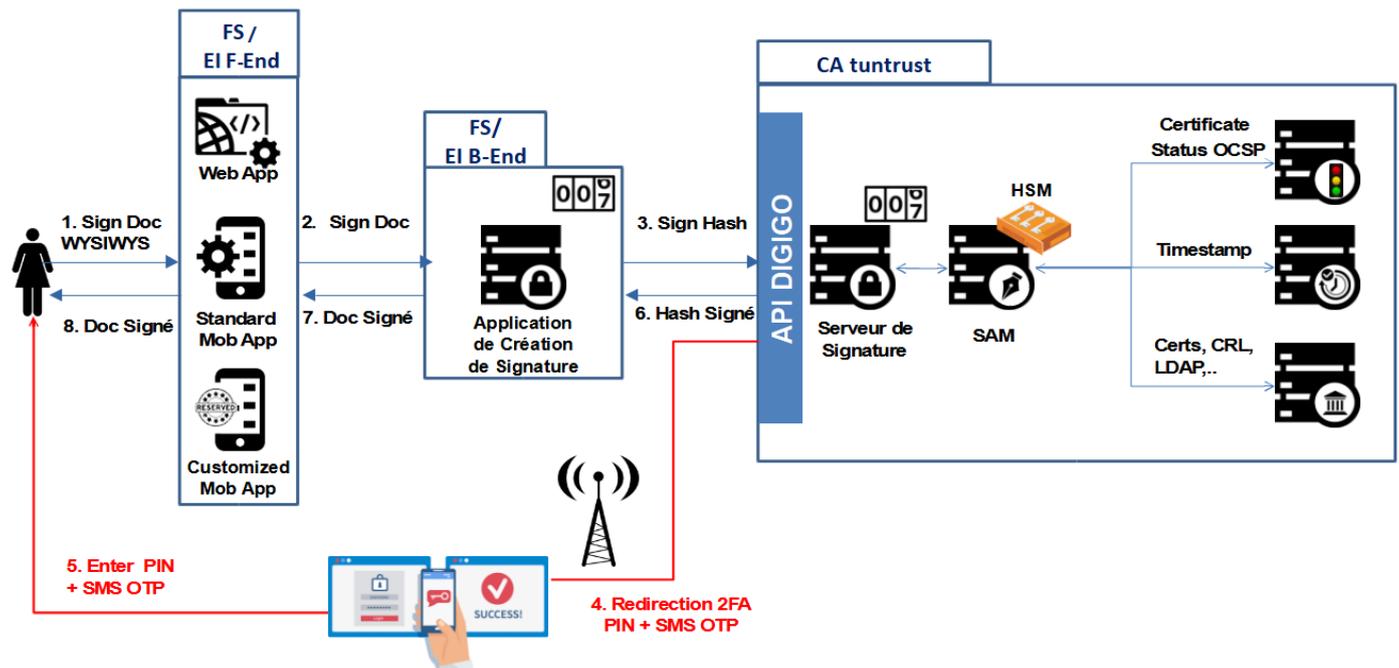
1.3 Formulaire

Identification physique (face-à-face) des demandeurs de certificat				
Nombre d'opérateurs			Nombre de guichets	
Liste des opérateurs	Nom et Prénom	Email (à associer au certificat digigo)	Numéro de téléphone	Numéro de CIN
Horaire de disponibilité des services				
Population cible				
Identification Vidéo des demandeurs de certificat				
Nombre d'opérateurs				
Liste des opérateurs	Nom et Prénom	Email (à associer au certificat DigiGo)	N° de téléphone	N° de CIN
Horaire de disponibilité de service				
Population Cible				
Paramètres relatifs à l'application d'enregistrement				
Adresse IP du serveur à autoriser				
Url de redirection (lors de la signature des demandes de certificats)				
Éditeur de l'Application d'Enregistrement (A remplir si l'ED n'est pas l'éditeur de la solution)				
Identifiant Unique				
Raison Sociale				

Adresse de l'éditeur			
N°, Rue, App		Code postal	
Ville		Gouvernorat	
Homologation de l'Application d'Enregistrement			
L'Application de Création de Signature est homologuée par TunTrust :	<input type="radio"/> Oui	<input type="radio"/> Non	
Si oui, fournir la date et l'identifiant de l'attestation d'homologation :			
Informations sur l'interlocuteur unique de l'éditeur			
Fonction			
Tél. professionnel		Mobile	
Email professionnel			

2 Intégration du Service de Signature à Distance

TunTrust offre le service de signature à distance schématisé selon la figure ci-dessous. TunTrust permet l'accès à son serveur de signature à distance à travers l'API DIGIGO (SCAL 2). Dans un premier temps, L'Entité d'Intégration dispose d'une Application de Création de Signature qui crée et transmet les données à signer (Hash) à TunTrust. Par la suite l'EI construit le document signé à partir des données signées remises par le serveur de signature de TunTrust. L'EI est reliée à TunTrust par un accord contractuel indiquant l'autorisation de son rôle en tant qu'EI de Signature et précisant clairement ses obligations et ses responsabilités.



L'Application de Création de Signature (ACS) se compose d'un Front-End qui fait l'interface avec le signataire en assurant le principe du WYSIWYS(*) et d'un Back-End qui permet de constituer le document signé. L'EI doit avoir le contrôle sur l'Application de Création de Signature Back-End qui sera reliée au serveur de signature de TunTrust à travers l'API de Signature à Distance DIGIGO.

L'Application de Création de Signature doit être homologuée par TunTrust conformément à la loi 83-2000 portant sur les échanges et le commerce électroniques. L'EI peut utiliser une ACS développée par un éditeur et ayant un certificat d'homologation valide fourni par TunTrust.

(*) WYSIWYS : Principe « What You Sign Is What You See »

2.1 Application de Création de Signature fournie par un Editeur

Ce tableau est à remplir uniquement si l'EI fait appel à un éditeur d'Application de Création de Signature pour la fourniture du service de signature à distance aux clients.

Editeur de l'Application de Création de Signature (A remplir si l'EI n'est pas l'éditeur)	
Identifiant Unique	
Raison Sociale	

Adresse de l'entité			
N°, Rue, App			
Code postal		Ville	
Gouvernorat		Pays	
Informations sur l'interlocuteur unique de l'éditeur			
Nom et Prénom			
Fonction			
Tél. professionnel		Mobile	
Email professionnel			

2.2 Homologation de l'Application de Création de Signature

Les formats de signature électronique doivent être conformes aux exigences ETSI pour les signatures électroniques listées ci-dessous :

1. **XAdES** (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)
2. **CAdES** (CMS Advanced Electronic Signature ETSI TS 101 733 and EN 319 122-1&2)
3. **ASiC** (Associated Signature Container ETSI TS 102 918 and EN 319 162-1&2)
4. **PAdES** (PDF Advanced Electronic Signature ETSI TS 102 778 and EN 319 142-1&2)

Types de signature fournis par l'Application de Création de Signature (Back-End)				
Formats de signature fournis par l'ACS	<input type="checkbox"/> PAdES	<input type="checkbox"/> XAdES	<input type="checkbox"/> CAdES	<input type="checkbox"/> ASiC
Packaging de signature fourni par l'ACS	<input type="checkbox"/> Enveloppée	<input type="checkbox"/> Enveloppante	<input type="checkbox"/> Détachée	
Niveau de signature fourni par l'ACS	<input type="checkbox"/> BASELINE-B	<input type="checkbox"/> BASELINE-T	<input type="checkbox"/> BASELINE-LT	<input type="checkbox"/> BASELINE-LTA
Homologation de l'Application de Création de Signature				
L'Application de Création de Signature est homologuée par TunTrust	<input checked="" type="radio"/> Oui		<input type="radio"/> Non	
Si oui, fournir la date et l'identifiant de l'attestation d'homologation				
Paramètres de l'Application de Création de Signature				
Adresse IP du serveur à autoriser côté TunTrust				
Adresse de redirection (redirectURI)				
Emplacement de l'hébergement du serveur				
Liste des comptes de test (emails associés aux certificats de test)				

2.3 Homologation de l'Application de Création de Cachet Électronique Visible

Cette section doit être remplie si l'EI va générer des cachets électroniques visibles en utilisant une application de génération de cachet **différente de celle de TunTrust**. Cependant, l'EI va utiliser l'API de signature Digigo et le certificat hébergé dans le HSM de TunTrust.

Homologation de l'Application de Création de Cachet Électronique Visible		
L'Application de Création de Cachet Électronique Visible est homologuée par TunTrust :	<input type="radio"/> Oui	<input type="radio"/> Non
Si oui, fournir la date et l'identifiant de l'attestation d'homologation		
Paramètres de l'Application de Création de Cachet Électronique Visible		
Adresse IP du serveur à autoriser côté TunTrust		