Documentation de l'API DIGIGO

Table des révisions

Version	Date	Nature de la révision	Section/Page
00	06/01/2020	Première rédaction	Toutes les pages
01	27/04/2020	Première révision	Sections 2 .3.3, 2.3.4, 2.3.6 -> 2.3.16, 3.1, 3.3, 3.4, 4, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 et 5.9
01.1	22/06/2020	Ajout d'autres webservices	Sections 2.3, 2.3.1 -> 2.3.4, 2.3.6 -> 2.3.17,3.1, 4, et 5
01.2	14/08/2020	Deuxième révision	Sections 2.3, 2.3.1 -> 2.3.4, 2.3.6 -> 2.3.17,3.1, 4, et 5
01.3	09/11/2020	Troisième révision	Sections 2.3, 2.3.1, 2.3.2, 2.3.6, 2.3.7, 2.3.8, 2.3.10, 2.3.11, 2.3.12, 2.3.13, 2.3.14, 2.3.15, 2.3.16, 2.3.17, 3.1, 3.3, et 3.6
01.4	08/03/2021	-Mise à jour du web service validate-identity -Modification au niveau du web service oauth2/authorize. -Correction URL du web service Timestamp. -Rectification du web service validate signature	Section 2.3.5 , 3.2 , 3.6, 4
01.5	17/03/2025	Mise à jour du web service revoke-certificate : changement au niveau du champ : revocationReason	De la page 30 à la page 32

Sommaire

1 Introduction

En vue de favoriser le développement des services de confiance numérique à l'échelle nationale et de créer un écosystème favorable à l'émergence de nouveaux acteurs dans le domaine de la certification électronique, l'**Agence Nationale de Certification Electronique - TunTrust** lance un appel de **partenariat** pour la création d'**Autorités d'Enregistrement Déléguées (AED)** qui contribueront à la commercialisation et la promotion des usages des services de confiance numérique nécessaires au développement de l'économie numérique.
Un modèle de contrat d'Autorité d'Enregistrement Déléguée est publié par TunTrust définissant le rôle des AED et précisant clairement leurs obligations et leurs responsabilités conformément aux exigences normatives et réglementaires appliquées par TunTrust.

Les objectifs majeurs du partenariat entre TunTrust et les AED couvrent essentiellement les points suivants :

- **Simplification des procédures par identification Vidéo des demandeurs de certificat.**

Les AED sont tenues 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). Désormais, il sera possible aux AED de remplacer le face-à-face physique avec le demandeur par un face-à-face vidéo conforme aux exigences techniques établies par TunTrust. Cette nouveauté permettra de simplifier la procédure d'enregistrement des demandes au profit des citoyens.

- **Promotion du Certificat Mobile DigiGO.**

Compte tenu du taux de pénétration de la téléphonie mobile et plus particulièrement des smartphones en Tunisie, le développement d'une solution d'authentification et de signature électroniques via le mobile devient une évolution naturelle des services de certification électronique offerts par TunTrust.

Dans ce contexte, TunTrust a lancé officiellement le Certificat Mobile DigiGO lors de la Troisième édition du Tunisia Digital Summit le 02 Avril 2019 à Tunis. Les AED seront alors les partenaires de TunTrust pour la promotion et la commercialisation de ce nouveau produit à l'échelle nationale.

- **Contribution à la digitalisation des administrations et des entreprises.**

TunTrust compte déléguer l'intégration des services d'authentification et de signature électronique aux autorités d'enregistrement déléguées afin de renforcer l'écosystème de la confiance numérique à l'échelle nationale. La startUp Act vient encore renforcer la mise en place de cet écosystème en instaurant un cadre propice à l'entreprenariat et à l'innovation. L'émergence de startup qui rempliront le rôle d'AED déléguée permettra de développer l'usage des services de confiance numérique dans le secteur bancaire, le secteur médical, le secteur de l'éducation et autres secteurs de services à valeur ajoutée.

1.1 Public cible

Il s'agit d'un document technique destiné au public cible suivant :

- Les autorités d'enregistrement déléguées devant transmettre les demandes de certificat de manière dématérialisée et sécurisée à TunTrust.
- Les fournisseurs de services qui ont besoin d'intégrer des services d'authentification et de signatures électroniques dans leur application. Les autorités d'enregistrement déléguées peuvent également être considérées comme des fournisseurs de services.

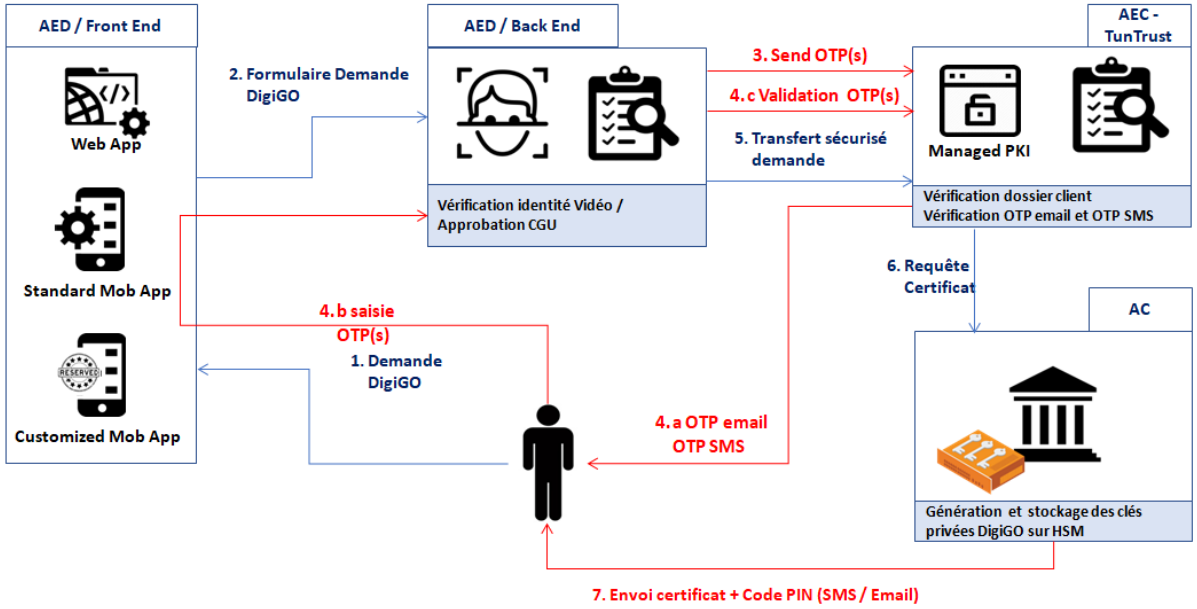
1.2 Objectif du document

Ce document fournit les spécifications de l'API Digigo Service. Cela inclut le format de données API, le protocole et autres spécifications connexes.

2 Enregistrement des demandes de certificat DigiGO

2.1 Identification vidéo des demandeurs de certificat

Cette section présente de manière sommaire les étapes du workflow d'enregistrement des demandes de certificat à travers une AED opérant une identification par vidéo.



1 Le demandeur utilise l'application Web ou Mobile fournie par l'AED pour remplir le formulaire de demande de certificat. Le formulaire doit contenir toutes les informations requises par TunTrust conformément au modèle fourni en annexe 1 du présent document.

2 Suite à la réception d'une demande de certificat, l'AED procède à l'identification de l'identité du demandeur par vidéo conformément aux exigences de TunTrust définies en annexe 2 du présent document.

3 Lors de la vérification vidéo, l'AED est appelée à vérifier l'adresse email du demandeur ainsi que son numéro de téléphone mobile à travers le service **aed-send-otp** de TunTrust.
Un OTP SMS et un OTP email sont envoyés directement par TunTrust au demandeur pour vérifier son contrôle sur le numéro de téléphone ainsi que sur l'adresse email.

4 Le demandeur saisit l'OTP SMS et l'OTP email qu'il a reçus à travers l'interface fournie par l'AED. Celle-ci vérifie la validité des OTP moyennant le web service **aed-validate-otp** de TunTrust. La transmission de la demande de certificat à TunTrust ne peut se faire qu'après validation avec succès de l'OTP SMS et de l'OTP email.

5 Après validation des OTP, la demande de certificat est transmise à TunTrust moyennant le web service **create-digigo-user**. Pour assurer l'authenticité et l'intégrité de la demande, la signature de l'AED est exigée pour chaque demande de certificat.

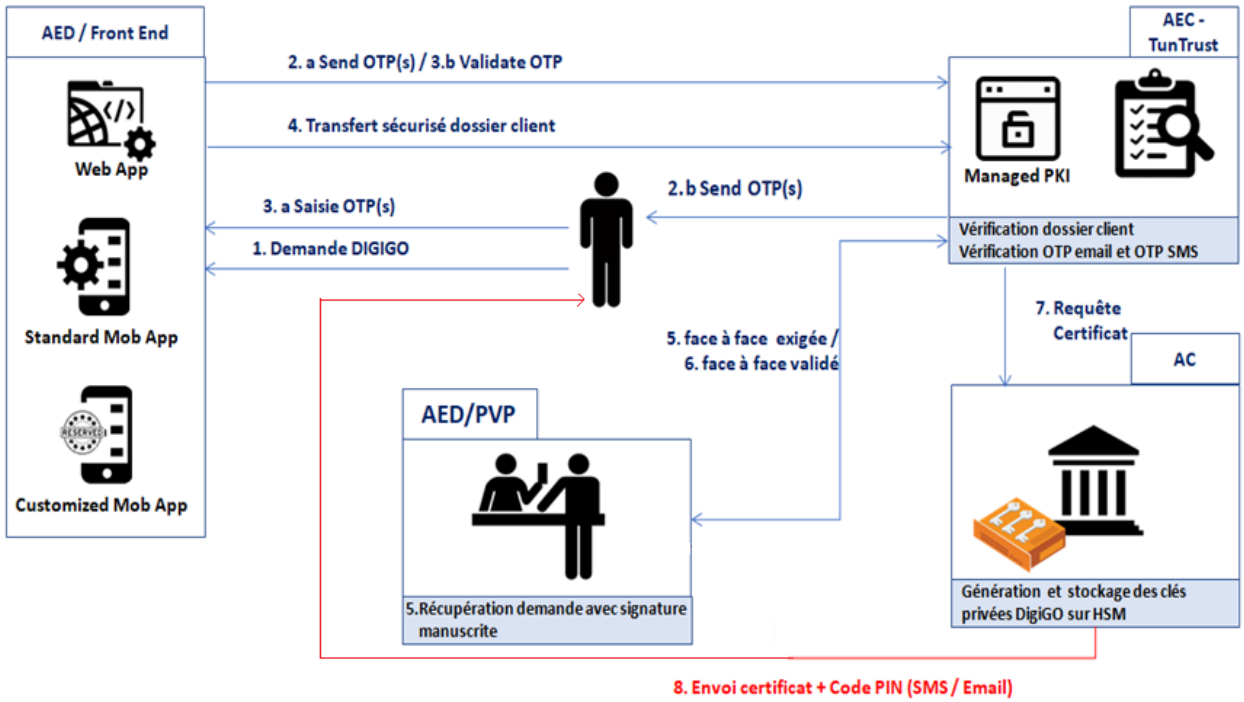
6 Après réception de la demande, TunTrust procède à son traitement. Un Web service **aed-request-status** de Tuntrust est disponible pour demander l'état d'une demande donnée.

7 Un certificat DigiGO est généré par TunTrust pour les demandes ayant été validées avec succès. Le code PIN du certificat est transmis directement au porteur de certificat sans passer par l'AED qui sera uniquement notifiée de la création du certificat et de l'envoi du code PIN au demandeur.

8 En cas de rejet de la demande, une notification de rejet est transmise à l'AED. TunTrust se réserve le droit de rejeter les demandes sans fournir des justificatifs à l'AED. Seul le demandeur a le droit de demander directement à TunTrust les motifs de rejet de la demande.

2.2 Identification face-à-face des demandeurs de certificat

Cette section présente de manière sommaire les étapes du workflow d'enregistrement des demandes de certificat à travers une AED opérant une identification face à face.



1 Le demandeur utilise l'application Web ou Mobile fournie par l'AED pour remplir le formulaire de demande de certificat. Le formulaire doit contenir toutes les informations requises par TunTrust conformément au modèle fourni en annexe 1 du présent document.

2 L'interface de demande de certificat de l'AED doit faire appel au service **aed-send-otp** de TunTrust pour la vérification de l'adresse email et du mobile du demandeur à travers des SMS OTP et email OTP.

3 Le demandeur doit saisir les OTP reçus sur son email et son mobile pour compléter sa demande de vérification. La transmission de la demande de certificat à TunTrust ne se fait qu'après validation de l'adresse email et du numéro de téléphone du demandeur moyennant le service **aed-validate-otp** fourni par TunTrust.

4 Après validation des OTP, la demande de certificat est transmise à TunTrust moyennant le web service **create-digigo-user**. Pour assurer l'authenticité et l'intégrité de la demande, la signature de l'opérateur de l'AED est exigée pour chaque demande de certificat.

5 Un Web service **aed-request-status** de Tuntrust est disponible pour demander l'état d'une demande donnée.

6 L'AED se charge de fixer un rendez-vous avec le demandeur pour établir une identification face-à-face. Le demandeur se déplace au bureau de L'AED le plus proche en présentant une copie de sa CIN. L'agent AED doit indiquer sur l'interface que le face à face physique avec le demandeur a été établi. Le web service **validateIdentity** permet de mettre à jour l'état d'une demande donnée suite à l'identification face à face avec le client chez l'AEC/l'AED.

7 Suite à cette indication, la génération du certificat sera faite et le code PIN du certificat sera alors automatiquement envoyé par TunTrust sur le mobile du demandeur.

8 En cas de rejet de la demande, une notification de rejet est transmise à l'AED. TunTrust se réserve le droit de rejeter les demandes et fournir des raisons du rejet à l'AED. Seul le demandeur a le droit de demander directement à TunTrust les motifs de rejet de la demande.

2.3 Les web services d'enregistrement de demande de certificat

Cette section concerne les AEDs qui souhaitent intégrer le service d'enregistrement des demandeurs de certificats électroniques.

DigiGo utilise des web services REST avec des appels HTTP encodés en JSON qui peuvent facilement être intégrés dans les plateformes des AEDs.

L'API DigiGo permet aux intégrateurs d'effectuer les fonctions d'enregistrement suivantes:

Nom du service	Fonction
aed-send-otp	Envoyer un mot de passe à usage unique sur le numéro de téléphone/ l'email du demandeur de certificat électronique.
aed-validate-otp	Valider un OTP saisi par le demandeur de certificat sur l'interface de l'AED.
create-digigo-user	Transmettre de manière sécurisée la demande de certificat à TunTrust après avoir validé les OTP envoyés.
upload-proof	Transmettre à TunTrust les pièces justificatives manquantes à la demande de certificat.
validate-identity	Vérifier l'identité physique du demandeur de certificat (face à face) effectué par l'agent de l'AED physique publique.
aed-request-status	Vérifier l'état en cours d'une demande de certificat.
aed-user-status	Vérifier l'état d'un utilisateur DigiGo.
revoke-certificate	Révoquer un certificat DigiGo.
unlock-pin	Débloquer le code PIN d'un certificat DigiGo.
request-affiliation	Associer un nouveau matricule fiscal à un utilisateur existant ayant un certificat DigiGO valide (non expiré et non révoqué).
approve-affiliation	Approuver l'affiliation pour un administrateur ou bien un collaborateur.
cancel-affiliation	Dissocier un matricule fiscal à un certificat DigiGo.
get-affiliation	Vérifier le status d'une demande d'affiliation déjà créé.
aed-user-info	Récupérer l'affiliation associée à un utilisateur.
change-affiliation	Changer l'affiliation d'un utilisateur de « ADMIN » à « collaborateur » ou le contraire.
get-quota	Récupérer le nombre de transactions associées à un porteur de certificat ou bien une AED.

2.3.1 aed-send-otp/{clientId}

Ce web-service permet l'envoi d'un OTP à l'adresse email et au numéro mobile du demandeur de certificat. L'objectif est de contrôler que le demandeur a bien le contrôle de l'adresse email qui sera mentionnée dans le certificat ainsi que le numéro de portable qui sera utilisé comme un deuxième facteur d'authentification en plus du code PIN du certificat. Un OTP est valide pour une durée de quinze (15) minutes.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-send-otp/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de **l'AED**
certType	OBLIGATOIRE	String	Ce paramètre indique le type de certificat à créer. Il doit contenir l'une des valeurs suivantes : • **PERSO** : personne physique sans attributs professionnels

Paramètre	Présence	Valeur	Description
			• **PRO** : personne physique avec des attributs professionnels • **SEAL** : personne morale (cachet électronique)
userId	OBLIGATOIRE Conditionnel	String	Ce paramètre contient l'identifiant de l'utilisateur de l'application de l'AED. Ce paramètre contient les valeurs suivantes : • Pour **certType = PERSO ou PRO,** le paramètre userId contient le numéro du CIN/ le passport/carte de séjour. • Pour **certType= SEAL**, le paramètre contient le matricule fiscal de l'organisation.
idType	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire pour certType égal à **PERSO**. Il permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
authDelivery	OBLIGATOIRE	Int	Ce paramètre indique le moyen de communication utilisé pour envoyer l'OTP : • **1 = SMS** • **2 = EMAIL**
phone	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire si **authDelivery =1.** Ce paramètre contient le numéro de téléphone sur lequel sera envoyé l'OTP.
email	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire si **authDelivery =2.** Ce paramètre contient l'adresse email sur laquelle sera envoyé l'OTP.
message	OPTIONNEL	String limité à 120 caractères	Ce paramètre contient le message à envoyer. La chaine doit contenir **la balise {0} afin de la remplacer par le code OTP**

Output :

Paramètre	Présence	Valeur	Description
txId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la transaction d'envoi OTP.
userId	OBLIGATOIRE Conditionnel	String	Ce paramètre contient l'identifiant du demandeur de certificat tel que défini dans l'input du tableau précédent.
authDelivery	OBLIGATOIRE	String	Ce paramètre indique le moyen de communication utilisé pour envoyer l'OTP tel que défini dans l'input du tableau précédent.
deliveryContact	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le numéro de téléphone ou l'email sur lequel un OTP a été envoyé.
deliverySendtime	OBLIGATOIRE Conditionnel	Timestamp	Ce paramètre contient la date et l'heure de l'envoi de l'OTP.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de la transaction de vérification de l'OTP défini comme suit : • **FAILURE** : l'envoi OTP a échoué • **WAITING** : En attente de la validation OTP par le demandeur du certificat.

Error codes :

Cas erreur	Status	Code	Description
La syntaxe du paramètre **clientId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is malformed.
La syntaxe du paramètre **certType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **certType** is malformed.

Cas erreur	Status	Code	Description
La syntaxe du paramètre **userId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is malformed.
La syntaxe du paramètre **authDelivery** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **authDelivery** is malformed.
La syntaxe du paramètre **phone** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **phone** is malformed.
La syntaxe du paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
La syntaxe du paramètre **message** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **message** is malformed.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **certType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **certType** is mandatory.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **userId** est invalide	INVALID REQUEST	400 (bad Request)	Invalid userId
Le paramètre **authDelivery** est vide	INVALID REQUEST	400 (bad Request)	The parameter **authDelivery** is mandatory.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **phone** est vide et authDelivery =1.	INVALID REQUEST	400 (bad Request)	The parameter **phone** is mandatory.
Le paramètre **email** est vide et authDelivery =2.	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
L'utilisateur est déjà enregistré.		400 (bad Request)	The user is already registred. • Pour **certType=PRO / PERSO,** vérifier que l'identifiant de l'utilisateur (**userId**) ou bien le téléphone (**phone**) ou bien l'(**email**) n'est pas déjà enregistré. • **Pour certType=SEAL,** vérifier que le téléphone (**phone**) ou bien **l'email** n'est pas déjà enregistré.
Le quota d'envoi d'OTP est atteint.	TOO MANY REQUEST	429	The quote of **email OTP** is reached | The quote of **SMS OTP** is reached. L'utilisateur peut avoir 03 tentatives pendant 05 minutes, après cela le compte est bloqué pendant 24 heures.
La gateway SMS est non disponible	SERVICE UNAVAILABLE	503	The **SMS gateway** is unavailable.
L'adresse IP utilisée est non déclarée pour l'AED	Forbidden	403	AED IP not authorized.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-send-otp/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{ "certType" : "PRO",
"userId" : "99999999",
"idType" : "CIN",
"authDelivery" : 1,
"phone" : "99111111"}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-send-otp
```

```
Content-Type: application/json
{
"txId" : " d7e5c39c-5be3-427a-8e10-f84e80f53c35",
"userId" : "99999999",
"authDelivery" : 1,
"status" : "WAITING"
"deliveryContact" : "99111111",
"deliverySendtime": 1587633950032,
}
```

2.3.2 aed-validate-otp/{clientId}/{txId}/{otp}

Ce web-service permet la validation de l'OTP saisi par le demandeur du certificat DIGIGO. Trois tentatives de validation sont autorisées. Après trois échecs, l'adresse email ou le numéro de portable utilisé pour la validation de l'OTP sera bloqué pour une durée d'une (01) heure.

Remarque : la durée du blocage de l'OTP est paramétrable par les administrateurs de TunTrust.

Input :
https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-validate-otp/{clientId}/{txId}/{otp}

Paramètre	Présence	Valeur	Description
txId	OBLIGATOIRE (URL)	String	Ce paramètre contient l'identifiant de la transaction effectuée avec l'AED.
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
otp	OBLIGATOIRE (URL)	String	L'OTP saisi par le demandeur de certificat au niveau de l'interface de l'AED.
certType	OBLIGATOIRE	String	Ce paramètre indique le type de certificat à créer. Il doit contenir l'une des valeurs suivantes : • **PERSO** : personne physique sans attributs professionnels • **PRO** : personne physique avec des attributs professionnels **SEAL** : personne morale (cachet électronique)
userId	OBLIGATOIRE Conditionnel	String	Ce paramètre contient l'identifiant de l'utilisateur de l'application de l'AED. Ce paramètre contient les valeurs suivantes : • Pour **certType = PERSO ou PRO,** le paramètre userId contient le numéro du CIN/ le passport/carte de séjour. • Pour **certType= SEAL**, le paramètre contient le matricule fiscal de l'organisation.
idType	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire pour certType égal à **PERSO**. Il permet d'identifier le type de la pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
authDelivery	OBLIGATOIRE	Int	Ce paramètre indique le moyen de communication utilisé pour envoyer l'OTP : **1 = SMS** **2 = EMAIL**
phone	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire si **authDelivery =1.** Ce paramètre contient le numéro de téléphone sur

			lequel sera envoyé l'OTP.
email	OBLIGATOIRE Conditionnel	String	Ce paramètre est obligatoire si **authDelivery =2.** Ce paramètre contient l'adresse email sur laquelle sera envoyé l'OTP.

Output :

Paramètre	Présence	Valeur	Description
txId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la transaction effectuée avec l'AED.
userId	OBLIGATOIRE Conditionnel	String	Ce paramètre contient l'identifiant de l'utilisateur de l'application de l'AED. Ce paramètre contient les valeurs suivantes : • **certType**= **PERSO** ou **PRO** le paramètre **userId** contient le numéro du CIN/ le passport/la carte de séjour • **certType**= **SEAL** contient le matricule fiscal de l'organisation.
authDelivery	OBLIGATOIRE	String	Ce paramètre indique le moyen de communication utilisé pour envoyer l'OTP tel que défini dans l'input de l'appel **aed-send-otp**. Selon le type d'OTP : • **1 = SMS** • **2= EMAIL**
deliveryContact	OBLIGATOIRE	String	Ce paramètre contient le numéro de téléphone ou l'adresse email ayant reçu l'OTP.
deliverySendtime	OBLIGATOIRE	Date time	Ce paramètre contient la date et l'heure de l'envoi de l'OTP.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de la transaction de vérification de l'OTP. Ce paramètre contient l'une des valeurs suivantes : • **SUCCESS (code : 200)** : la vérification OTP effectuée avec succès • **FAILURE** : la vérification OTP a échoué • **WAITING** : En attente de validation OTP par le demandeur du certificat. • **EXPIRED** : la durée de vie de l'OTP a expirée.

Error Codes :

Cas erreur	Status	Code	Description
Le paramètre **txId** est invalide	INVALID REQUEST	400 (bad Request)	The transaction **txId** is invalid.
Nombre d'erreur autorisé dépassé	INVALID REQUEST	400 (bad Request)	User account is blocked. Too Many Failed Attempts.
Le paramètre **txId** est vide	INVALID REQUEST	400 (bad Request)	The transaction **txId** is mandatory.
La syntaxe du paramètre **clientId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is malformed.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **otp** est vide	INVALID REQUEST	400 (bad Request)	The **otp** is mandatory.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-validate-otp/694b650c-eceb-4765-94f7-d170b4a1247c/d7e5c39c-5be3-427a-8e10-f84e80f53c35/4da15a1
Host: digigo.tuntrust.tn
```

```
Content-Type: application/json
{ "certType" : "PRO",
"userId" : "99999999",
"idType" : "CIN",
"authDelivery" : 1,
"phone" : "99111111"}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-validate-otp
Content-Type: application/json
{
"txId" : "d7e5c39c-5be3-427a-8e10-f84e80f53c35",
"userId" : "99999999",
"authDelivery" : 1,
"status" : "SUCCESS"
"DeliveryContact" : "99111111",
"deliverySendtime": 1587374130000"}
```

2.3.3 create-digigo-user/{clientId}

Ce web-service est utilisé par l'AED pour transmettre de manière sécurisée la demande de certificat à TunTrust. Ce service ne peut être appelé qu'après avoir validé l'OTP SMS et l'OTP Email du demandeur de certificat. Dans le cas de l'identification vidéo, l'AED doit fournir l'URL de téléchargement de la vidéo. Toutes les informations transmises à TunTrust à travers cet appel doivent être signées par l'opérateur de l'AED.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/create-digigo-user/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.
certType	OBLIGATOIRE	String	Ce paramètre contient l'une des valeurs suivantes : • **PERSO** : personne physique sans attributs professionnels • **PRO :** personne physique avec des attributs professionnels • **SEAL :** personne morale (cachet électronique)
txIdPhone	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP de type SMS.
txIdEmail	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP de type EMAIL.
Informations sur l'organisation			
country	OBLIGATOIRE	String 2 lettres (ISO3166)	Ce paramètre contient le code du pays (**ISO3166**) : • Pour **certType=PRO / SEAL**, le code correspond au pays d'enregistrement de l'entité • Pour **certType=PERSO**, le code correspond à la nationalité du demandeur de certificat
organisationId	OBLIGATOIRE Conditionnel	String Alphanumérique <=30 caractères	Ce champ est obligatoire uniquement dans le cas de certificats de type **PRO et SEAL (certType=PRO / SEAL).** Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient le matricule fiscal de l'organisation sous ce format : 7

Paramètre	Présence	Valeur	Description
			chiffres et une lettre. Il est validé par un algorithme de vérification du format.
Organisation	OBLIGATOIRE Conditionnel	String <= 200 caractères	Ce paramètre correspond à la raison sociale de l'organisation. Ce champ est obligatoire uniquement dans le cas de certificats de type **PRO et SEAL.**
taxIdentifierFile	OBLIGATOIRE Conditionnel	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce champ est obligatoire uniquement dans le cas de certificats de **type PRO, SEAL** avec **country TN.** Ce paramètre correspond à la pièce jointe relative à la carte d'identification fiscale
taxIdentifierFileType	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le type de document carte d'identité fiscale. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
nationalBusinessRegisterFile	OBLIGATOIRE Conditionnel	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce champ est obligatoire uniquement dans le cas de certificats de **type PRO, SEAL (certType=PRO / SEAL).** Ce paramètre correspond à la pièce jointe relative au registre national des entreprises.
nationalBusinessRegisterFile Type	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le type de document RNE. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
Informations sur le représentant légal			
legalRepresentativeName	OBLIGATOIRE Conditionnel	String <= 40 lettres	Ce champ est obligatoire uniquement dans le cas de certificats de type **PRO, SEAL.** Ce paramètre contient le nom du représentant légal.
legalRepresentativeFirstnam e	OBLIGATOIRE Conditionnel	String <= 40 lettres	Ce champ est obligatoire uniquement dans le cas de certificats de **type PRO/SEAL.** Ce paramètre contient le prénom du représentant légal.
legalRepresentativeBirthdate	OBLIGATOIRE Conditionnel	Date	Ce champ est obligatoire uniquement dans le cas des certificats de **type PRO/SEAL.** Ce paramètre contient la date de naissance du représentant légal.
legalRepresentativeIdentityT ype	OBLIGATOIRE Conditionnel	String	Ce paramètre contient trois types de valeurs : • CIN • PASSEPORT • CARTESEJOUR Ce champ est obligatoire uniquement dans le cas de **certificats de type PRO/SEAL.**
legalRepresentativeId	OBLIGATOIRE Conditionnel	String	Ce paramètre correspond au numéro de l'identité du représentant légal (numéro CIN, numéro passeport, numéro carte de séjour). Ce champ est obligatoire uniquement dans le cas de certificats **de type PRO/SEAL.**

Paramètre	Présence	Valeur	Description
			Si (**legalRepresentativeIdentityType =CIN**), le paramètre **legalRepresentativeId = 8 chiffres** Sinon le paramètre **legalRepresentativeId: Alphanumérique <=16 caractères**
legalRepresentativePhoneNumber	OBLIGATOIRE Conditionnel	String (format phone)	Ce paramètre correspond au numéro de téléphone mobile du représentant légal. Ce champ est obligatoire uniquement dans le cas de certificats **de type PRO/ SEAL .**
legalRepresentativeEmail	OBLIGATOIRE Conditionnel	String (syntaxe email)	Ce paramètre correspond à l'adresse email du représentant légal. Ce champ est obligatoire uniquement dans le cas de certificats **de type PRO/ SEAL.**
legalRepresentativeIdentityFile	OBLIGATOIRE Conditionnel	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond à une pièce jointe contenant la pièce d'identité du représentant légal (CIN, passport, carte de séjour). Ce champ est obligatoire uniquement dans le cas de certificats **de type PRO/ SEAL.**
legalRepresentativeIdentityFileType	OBLIGATOIRE Conditionnel	string	Ce paramètre contient le type de document carte d'identité fiscal. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
Informations du demandeur de certificat / responsable cachet			
subscriberName	OBLIGATOIRE	String <= 40 caractères	Ce paramètre contient le nom du demandeur du certificat pour les certificats de type **PERSO /PRO** et contient le prénom du responsable cachet en cas de certificat **SEAL.**
subscriberFirstname	OBLIGATOIRE	String <= 40 caractères	Ce paramètre contient le prénom du demandeur du certificat pour les certificats PERSO, PRO **(certType =PERSO /PRO**) et contient le prénom du responsable cachet en cas de certificat SEAL **(certType = SEAL).**
subscriberBirthdate	OBLIGATOIRE	Date/long	Ce paramètre contient la date de naissance du demandeur du certificat pour les certificats de type **PERSO /PRO** et contient le prénom du responsable cachet en cas de certificat **SEAL.**
subscriberIdentityType	OBLIGATOIRE	String	Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
subscriberId	OBLIGATOIRE	8 chiffres subscriberIdentityType= CIN sinon Alphanumérique <=16 caractères	Ce paramètre correspond au numéro de l'identité du demandeur du certificat (numéro CIN, numéro passeport, numéro carte de séjour). Si **(subscriberIdentityType=CIN)** le paramètre subscriberId = 8 chiffres. Sinon le paramètre subscriberId : Alphanumérique <=16 caractères
subscriberPhone	OBLIGATOIRE	Chiffres (format phone)	Ce paramètre correspond au numéro téléphone mobile du demandeur du certificat pour les certificats PERSO, PRO **(certType=PERSO /PRO)** et contient le numéro de téléphone mobile du responsable cachet en cas de certificat SEAL **(certType= SEAL).**

Paramètre	Présence	Valeur	Description
subscriberEmail	OBLIGATOIRE	String (syntaxe email)	Ce paramètre contient l'adresse email du demandeur du certificat pour les certificats PERSO, PRO **(certType=PERSO /PRO)** et contient le prénom du responsable cachet en cas de certificat SEAL **(certType= SEAL).**
subscriberIdentityFile	OBLIGATOIRE	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond à une pièce jointe contenant la pièce d'identité du demandeur du certificat pour les certificats PERSO, PRO **(certType =PERSO /PRO)** et contient le prénom du responsable cachet en cas de certificat SEAL **(certType = SEAL).**
subscriberIdentityFileType	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
screenshotFile1	OBLIGATOIRE Conditionnel	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond à une screenshot effectuée par l'opérateur de l'AED lors de la présentation du recto de la pièce d'identité du demandeur du certificat lors de l'interview vidéo.
screenshot1FileType	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le type de document screenshot1. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
screenshotFile2	OBLIGATOIRE Conditionnel	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond à une screenshot effectuée par l'opérateur de l'AED lors de la présentation du verso de la pièce d'identité du demandeur du certificat lors de l'interview vidéo.
screenshot2FileType	OBLIGATOIRE Conditionnel	String	Ce paramètre contient le type de document screenshot2. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
requestSignature	OBLIGATOIRE	String/base 64	Ficher texte contenant tous les autres champs en **JSON** signé en Xades/Envelopping par un Opérateur de **l'AED.**
urlVideo	OBLIGATOIRE Conditionnel	String	Ce paramètre contient l'URL de vidéo. Ce paramètre devient obligatoire si l'AED effectue l'identification par vidéo. Le format de la vidéo est MP4. Le codec vidéo est H264. La taille de la vidéo ne doit pas dépasser 2 Go.
videoHash	OBLIGATOIRE Conditionnel	String	Haché de la vidéo au format **SHA-256.** Ce paramètre devient obligatoire si l'AED effectue l'identification par vidéo.

put :

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la requête émise par le client.
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'**AED**.
userId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'utilisateur de l'application de l'AED.
requestStatus	OBLIGATOIRE	String	Ce paramètre contient l'une des valeurs suivantes : • **ONGOING** (code 202) : la requête est en attente de validation. Par défaut ce champ prend la valeur « **ONGOING** » si tous les champs sont conformes. • **REJECTED** : en cas d'échec de création de l'utilisateur
requestTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de l'enregistrement de la requête.
message	OBLIGATOIRE Conditionnel	String	Si requestStatus=REJECTED

Error Codes :

Type d'erreur	Code d'erreur	Message d'erreur
Le paramètre **clientId** est invalide	400 (bad Request)	The parameter **clientId** is malformed.
Le paramètre **certType** est invalide	400 (bad Request)	The parameter **certType** is malformed.
Le paramètre **txIdPhone** est invalide	400 (bad Request)	The parameter **txIdPhone** is malformed.
Le paramètre **txIdEmail** est invalide	400 (bad Request)	The parameter **txIdEmail** is malformed.
Le paramètre **country** est invalide	400 (bad Request)	The parameter **country** is malformed.
Le paramètre **organisationId** est invalide	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** n'est pas enregistré au RNE	403	The **organisationId** is not registred in the RNE.
Le paramètre **organisation** est invalide	400 (bad Request)	The parameter **organisation** is malformed.
Le paramètre **taxIdentifierFile** est invalide	400 (bad Request)	The parameter **taxIdentifierFile** is malformed.
Le paramètre **nationalBusinessRegisterFile** est invalide	400 (bad Request)	The parameter **nationalBusinessRegisterFile** is malformed.
Le paramètre **legalRepresentativeName** est invalide	400 (bad Request)	The parameter **legalRepresentativeName** is malformed.
Le paramètre **legalRepresentativeFirstname** est invalide	400 (bad Request)	The parameter **LegalRepresentativeFirstname** is malformed.
Le paramètre **legalRepresentativeBirthdate** est invalide	400 (bad Request)	The parameter **legalRepresentativeBirthdate** is malformed.
Le paramètre **legalRepresentativeIdentityType** est invalide	400 (bad Request)	The parameter **legalRepresentativeIdentiType** is malformed.
Le paramètre **legalRepresentativeId** est invalide	400 (bad Request)	The parameter **legalRepresentativeId** is malformed.
Le paramètre **legalRepresentativePhoneNumber** est invalide	400 (bad Request)	The parameter **legalRepresentativePhoneNumber** is malformed.

Le paramètre **legalRepresentativeEmail** est invalide	400 (bad Request)	The parameter **legalRepresentativeEmail** is malformed.
Le paramètre **legalRepresentativeIdentityFile** est invalide	400 (bad Request)	The parameter **legalRepresentativeIdentityFile** is malformed.
Le paramètre **subscriberName** est invalide	400 (bad Request)	The parameter **subscriberName** is malformed.
Le paramètre **subscriberFirstname** est invalide	400 (bad Request)	The parameter **subscriberFirstname** is malformed.
Le paramètre **subscriberBirthdate** est invalide	400 (bad Request)	The parameter **subscriberBirthdate** is malformed.
Le paramètre **subscriberEmail** est invalide	400 (bad Request)	The parameter **subscriberEmail** is malformed.
Le paramètre **subscriberIdentityFile** est invalide	400 (bad Request)	The parameter **subscriberIdentityFile** is malformed.
Le paramètre screenshot1File est invalide	400 (bad Request)	The parameter **screenshot1File** is malformed.
Le paramètre screenshot2File est invalide	400 (bad Request)	The parameter **screenshot2File** is malformed.
Le paramètre **subscriberId** est invalide	400 (bad Request)	The parameter **subscriberId** is malformed.
Le paramètre **subscriberIdentityFileType** est invalide	400 (bad Request)	The parameter **subscriberIdentityFileType** is malformed.
Le paramètre **urlVideo** est invalide	400 (bad Request)	The parameter **urlVideo** is malformed.
Le paramètre **requestSignature** est invalide	400 (bad Request)	The parameter **requestSignature** is invalid.
L'adresse email du demandeur du certificat est déjà enregistrée	403	The email address ****** is already registred.
Le numéro de portable du demandeur du certificat est déjà enregistré	403	The phone number ***** is already registred.
L'identifiant du demandeur du certificat est déjà enregistré	403	**subscriberId** is already registred.
Les OTPs envoyés ne sont pas encore vérifiés par le demandeur du certificat.	401	The OTPs are not validated by the subscriber.
Erreur interne	500	The server encounters an unexpected condition.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/create-digigo-user/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
       "txIdEmail" :"5460a4b6-7b1a-47dd-8be5-dbc5c98a4279" ,
      "txIdPhone" :"d7e5c39c-5be3-427a-8e10-f84e80f53c35" ,
       "certType" :"PRO" ,
      "country" :"TN" ,
      "organisation" :"ANCE" ,
      "organisationId"  :"1111111A" ,
      "taxIdentifierFile":" TAAAACXBIWXMAAA9hAA…" ,
      "taxIdentifierFileType" :"image/png" ,
       "nationalBusinessRegisterFile" :"iVBORw0KGgoA…" ,
      "nationalBusinessRegisterFileType" :"image/png" ,
      "legalRepresentativeName" :"ben flen" ,
      "legalRepresentativeFirstname" :" flen" ,
      "legalRepresentativeBirthdate" :"1577457071000" ,
      "legalRepresentativeIdentityType" :"CIN" ,
```

```
        "legalRepresentativeId" :"01234567" ,
        "legalRepresentativePhoneNumber" :"99999999" ,
        "legalRepresentativeEmail" :"flen@certification.tn" ,
        "legalRepresentativeIdentityFile" : "iVBOR…" ,
        "legalRepresentativeIdentityFileType" :"image/png" ,
        "subscriberName" :" ben flen" ,
        "subscriberFirstname" :"flen" ,
        "subscriberBirthdate" :"1577457071000" ,
        "subscriberIdentityType" :"CIN" ,
        "subscriberId" :" 99999999" ,
        "subscriberPhone" :"9911111" ,
        "subscriberEmail" :"flen@certification.tn" ,
        "subscriberIdentityFile" : "iVBORw0KGgoAA…" ,
        "subscriberIdentityFileType" :"image/png" ,
        "screenshot1File" : "tVuofciVBORw0KGgoAA…" ,
        "screeshot1FileType" :"image/png" ,
        "screenshot2File" : "FRTOIVSETPOvsd…" ,
        "screeshot2FileType" :"image/png" ,
        "requestSignature" :"+PGRzOlNpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDo…" ,
        "urlVideo" :"https://www...",
        "videoHash" : "WdPaUpvZEhSd2N6b3ZMM2QzZHk1NWIzV"
              }
```


Exemple de réponse :


```
HTTP/1.1 200 Found
{
"requestId" : "7742a7d7-8575-44a2-954a-e8c04f0013e1",
"clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
"userId " : "99999999",
"requestStatus" : "ONGOING",
"requestTimestamp" : "1579594591268"
}
```


2.3.4 upload-proof/{clientId}/{requestId}

Ce web-service permet à l'AED de transmettre à TunTrust les pièces justificatives manquantes à la demande de certificat. Les tailles des fichiers justificatifs ne doivent pas dépasser 1Mo/fichier.

Input :

https:// digigo.tuntrust.tn /tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/upload-proof/{clientId}/{requestId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.
requestId	OBLIGATOIRE (URL)	String	Ce paramètre contient l'identifiant de la demande de certificat.
legalRepresentativeIdentityFile	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre contient le document **legalRepresentativeIdentityFile** à mettre à jour.
legalRepresentativeIdentityFileType	OPTIONAL	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif

Paramètre	Présence	Valeur	Description
subscriberIdentityFile	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre contient le document **subscrberIdentityFile** à mettre à jour.
subscriberIdentityFileType	OPTIONAL	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
screenshotFile1	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond au document screenshot1 à mettre à jour.
screenshot1FileType	OPTIONAL	String	Ce paramètre contient le type de document screenshot1. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
screenshotFile2	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre correspond au document screenshot2 à mettre à jour.
screenshot2FileType	OPTIONAL	String	Ce paramètre contient le type de document screenshot2. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
legalRepresentativeIdentityFile	OPTIONAL	Fichier (string)pdf, jpg, gif, png, bmp, tif	Ce paramètre contient le document **legalRepresentativeIdentityFile** à mettre à jour.
legalRepresentativeIdentityFileType	OPTIONAL	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
taxIdentifierFile	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre contient le document **taxIdentifierFile** à mettre à jour.
taxIdentifierFileType	OPTIONAL	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient

Paramètre	Présence	Valeur	Description
			l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
nationalBusinessRegisterFile	OPTIONAL	Fichier (string) pdf, jpg, gif, png, bmp, tif	Ce paramètre contient le document **NationalBusinessRegisterFile** à mettre à jour.
nationalBusinessRegisterFileType	OPTIONAL	String	Ce paramètre contient le type de document d'identification de l'utilisateur. Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
urlVideo	OPTIONAL	String	Ce paramètre contient le document **urlVideo** à mettre à jour.
videoHash	OPTIONAL	String	Haché de la vidéo au format SHA-256.
requestSignature	OBLIGATOIRE	String/ base64	Ficher texte contenant tous les autres champs en JSON signé en Xades / Envelopping par un Opérateur de l'AED

Output :

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la demande de certificat.
requestStatus	OBLIGATOIRE	String	Ce paramètre correspond à l'état de téléchargement des pièces jointes effectué par l'agent de l'AED. Ce paramètre contient deux types de valeurs : • **ONGOING** (code 202): Téléchargement effectué avec succès. • **FAILURE** : Téléchargement a échoué.
verificationTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de réception des documents requis.

Error Codes :

Type d'erreur	Code d'erreur	Message d'erreur
Le champ requestId ne correspond pas au clientId.	401	Unauthorized: The clientId is not authorized to update the requestId.
Le fichier ****** est invalide	400 (bad Request)	The type of file ******* is not authorized.
Le fichier ****** a dépassé la taille maximale autorisée.	400 (bad Request)	The file ****** has exceeded the maximum allowed size.
Le compte de l'utilisateur est déjà validé	400 (bad Request)	User already validated
Le champ **requestSignature** est vide	400 (bad Request)	**requestSignature** is mandatory
Le champ **requestSignature** est invalide	400 (bad Request)	**requestSignature** invalid
Signature invalide	400 (bad Request)	sent data and signed data must be identical
La demande de certificat est inexistante	404	The request n° **requestId** is not found.
Erreur interne	500	The server encounters an unexpected condition.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/upload-proof/694b650c-eceb-4765-94f7-d170b4a1247c/7742a7d7-8575-44a2-954a-e8c04f0013e1
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"subscriberIdentityFile":"/9j/4RZlRXhpZgAATU0AKgAAAAgADAEAAAMAAAABCbUAAAEBAAMAAAACA…" ,
"subscriberIdentityFileType" :"image/jpg" ,
"requestSignature":"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj…",
"urlVideo" :"https://www...",
"videoHash" : "WdPaUpvZEhSd2N6b3ZMM2QzZHk1NWIzV"
}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
"requestStatus" : "ONGOING",
"clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
"requestId" : "7742a7d7-8575-44a2-954a-e8c04f0013e1",
"verificationTimestamp" : "1583486466000"
}
```

2.3.5 validate-identity/{clientId}

Ce web-service permet de vérifier l'identité physique du demandeur de certificat (face à face) effectué par l'agent de l'AED physique publique suite validation de la demande par l'agent de Tuntrust.

Input :

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la demande de certificat qui doit être en état « VALID »
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.
timestampIdentityVerification	OBLIGATOIRE	Timestamp	Ce paramètre contient la date et l'heure de vérification de l'identité du demandeur de certificat. **[UTC time mill sec UNIX]**
ProofFile	OBLIGATOIRE	Fichier (bytes) Les formats suivants sont uniquement acceptés : pdf, jpeg, jpg, gif, png Un contrôle sur les fichiers exécutables est à prévoir.	Ce paramètre contient un document signé par le demandeur de certificat après la vérification effectuée par l'agent de l'AED physique.
proofFileType	OBLIGATOIRE	string	Ce paramètre contient le type de document, Il contient l'une des valeurs suivantes : • image/jpg • image/gif • image/png • application/pdf • image/bmp • image/tif
txSignature	OBLIGATOIRE	String	Ce paramètre contient la signature par le certificat de l'agent de l'AED physique de tous les champs de cette transaction.

Output :

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la demande de certificat.
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'AED.
requestStatus	OBLIGATOIRE	String	Ce paramètre contient l'état de l'identification effectuée par l'agent de l'AED. Ce paramètre peut être l'une des valeurs suivantes: • **VALID** (code 202): en cas d'identification physique du demandeur du certificat. Le changement à cet état est effectué avec l'une des trois manières suivants : ○ Opérateur de TunTrust (suite à la visualisation et la validation de la vidéo d'identification) ○ Opérateur de TunTrust si le face-à-face est effectué à TunTrust ○ Opérateur de l'AED publique respons able de l'identification via face-à-face • **REJECTED** : la demande de certificat est rejetée par l'opérateur TunTrust • **MISSING_INFO** : la demande de certificat nécessite des vérifications supplémentaires (exemple : fichier contenant le CIN est invalide/ face à face requis). • **ONGOING** : la demande de certificat est en attente de validation. • **GENERATING**: Génération du certificat en cours par l'agent AED Physique.
Message	OBLIGATOIRE	String	Message informatif
verificationTim estamp	OBLIGATOIRE	Timestamp	Ce paramètre contient la date et l'heure de vérification de l'identité du demandeur de certificat. **[UTC time mill sec UNIX]**

Error Codes :

Type d'erreur	Code d'erreur	Message d'erreur
le champ **requestId** ne correspond à aucune demande enregistrée.	404	the **requestId** does not exist.
le champ **requestId** est vide	400 (bad Request)	the field **requestId** is mandatory.
le champ **clientId** est vide	400 (bad Request)	the field **clientId** is mandatory.
le champ **timestampIdentityVerification** est vide	400 (bad Request)	the field **timestampIdentityVerification** is mandatory.
Le **clientId** n'est pas de type administrateur et le champ proofFile est vide	400 (bad Request)	the **clientId** is not admin : the field **proofFile** is mandatory.
le champ **txSignature** est vide	400 (bad Request)	the field **txSignature** is mandatory.
le champ **timestampIdentityVerification** est invalide	400 (bad Request)	the field **timestampIdentityVerification** is malformed.
Le **clientId** n'est pas de type administrateur (AEC) et le champ proofFile est de format invalide	400 (bad Request)	the **clientId** is not admin : the field **proofFile** is malformed.
la signature **txSignature** est invalide	400 (bad Request)	the signature **txSignature** is invalid.
erreur interne	500	the server encounters an unexpected condition.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/validate-identity/694b650c-eceb-4765-94f7-d170b4a9807c

{
```

```
"requestId":"69f5c9d4-7981-4551-a7f8-70ba8e03aa86",
"timestampIdentityVerification":"1612450507000",
"proofFile":"JVBERi0xLjQKJdPr6eEKMSAwIG9iago8PC9DcmVhdG9yIChNb3ppbGxhLzUuMCBcKFgxMTsgTGludXgge
Dg2XzY0XCkgQXBwbGVXZWJLaXQvNTM3LjM2IFwoS0hUTUwsIGxpa2UgR2Vja29cKSBDaHJvb…",
"proofFileType":"application/pdf",
"requestSignature":"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZG…"
}
```


Exemple de réponse :


```
HTTP/1.1 200 Found

{

"requestSatus":"GENERATING",
"clientId":"694b650c-eceb-4765-94f7-d170b4a9807c",
"requestId":"69f5c9d4-7981-4551-a7f8-70ba8e03aa86",
"message":null,
"verificationTimestamp":1612450507000,

}
```


2.3.6 aed-request-status/{clientId}/{requestId}

Ce Web Service permet à l'AED de vérifier l'état d'une demande de création de certificat par l'agent de l'AED. Il peut être appelé après l'enregistrement de la demande de création de l'utilisateur.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-request-status/{clientId}/{requestId}

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE (URL)	String	Ce paramètre contient l'identifiant de la demande de certificat.
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.

Output :

Paramètre	Présence	Valeur	Description
requestId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la demande de certificat.
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'**AED**.

requestStatus	OBLIGATOIRE	String	Ce paramètre contient l'une des valeurs suivantes :
			• **ONGOING** (code 202) : la requête est en attente de validation. Par défaut ce champ prend la valeur « **ONGOING** » si tous les champs sont conformes.
			• **REJECTED** : en cas d'échec de création de l'utilisateur
			• **VALID** (code 202): en cas d'identification physique du demandeur du certificat. Le changement à cet état est effectué avec l'une des trois manières suivantes :
			  • Opérateur de TunTrust (suite à la visualisation et la validation de la vidéo d'identification)
			  • Opérateur de TunTrust si le face-à-face est effectué à TunTrust

			• Opérateur de l'AED publique responsable de l'identification via face-à-face • **MISSING_INFO**: la demande de certificat nécessite des vérifications supplémentaires (exemple : fichier contenant le CIN est invalide) • **EMAILNOTACCEPTED :** l'adresse email du demandeur du certificat n'est pas acceptée. • **FACETOFACEREQUIRED :** une identification face à face est exigée • **GENERATING:** le certificat est en cours de génération. • **GENERATED:** Le certificat a été généré
message	OBLIGATOIRE	String	Selon la valeur du champ **requestStatus**, ce champ contient l'une des valeurs suivantes : • **requestStatus=ONGOING : message=**The request is waiting for validation. • **requestStatus=REJECTED** : **message=** The request has been rejected for the reason: *******. • **requestStatus=VALID : message=**The face to face identification is validated by TunTrust operator. • **requestStatus=MISSING_INFO**: **message=**The request is missing a file. • **requestStatus=FACETOFACEREQUIRED : message=**A face to face identification is required. • **requestStatus=EMAILNOTACCEPTED : message=The email address of subcriber is not accepted by TunTrust.** • **requestStatus=GENERATING: message=**The certificate issuance is in progress. • **requestStatus=GENERATED: message=**The certificate is issued.
verificationTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de la création du user.
freeMessage	OBLIGATOIRE	String	Un champs text libre ajouté par l'opérateur ANCE afin de bien expliquer le problème en cas de MissingInfo .

Error Codes:

Error case	Status Code	Error	Error Description
Le paramètre "**clientId**" est vide	400 (bad Request)	invalid_request	Missing parameter **clientId**
Le paramètre "**clientId**" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **clientId**
Le paramètre " **requestId** " est vide	400 (bad Request)	invalid_request	Missing parameter **requestId**
Le paramètre " **requestId** " est invalide	400 (bad Request)	invalid_request	Invalid parameter **requestId**

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-request-status/694b650c-eceb-4765-94f7-d170b4a1247c/7742a7d7-8575-44a2-954a-e8c04f0013e1
```

```
HTTP/1.1
```

Exemple de réponse :

```
HTTP/1.1 200 Found

{ "clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",

  "requestId" : "7742a7d7-8575-44a2-954a-e8c04f0013e1",

  "requestStatus" : "MISSING_INFO",

  "message" : " The request is missing a file. ",

  "verificationTimestamp" : "1583486466000",

  "freeMessage": "MANQUE PATENTE"

}
```

2.3.7 aed-user-status/{clientId}/{userId}/{idType}/{email}

Ce Web Service permet à l'AED de vérifier l'état d'inscription DigiGo d'un utilisateur quelconque.

Input :

https:// digigo.tuntrust.tn /tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-user-status/{clientId}/{userId}/{idType}/{email}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.
userId	OBLIGATOIRE (URL)	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
idType	OBLIGATOIRE (URL)	String	Il permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : ○ **CIN** ○ **PASSEPORT** ○ **CARTESEJOUR**
email	OBLIGATOIRE (URL)	String	Ce paramètre contient l'adresse email qui correspond au compte utilisateur DigiGo.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'**AED initiale**.
requestId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de la demande de certificat.
requestStatus	OBLIGATOIRE	String	Ce paramètre contient l'une des valeurs suivantes : • **ONGOING** (code 202) : une requête pour (userId, email) est créée et en attente de validation. Par défaut ce champ prend la valeur « **ONGOING** » si tous les champs sont conformes. • **REJECTED** : une requête pour (userId, email) est créée et a été rejetée. • **VALID** (code 202): une requête pour (userId, email) est créée et a été validée par les

			opérateurs de TunTrust. • **MISSING_INFO**: une requête pour (userId, email) est créée et nécessite des vérifications supplémentaires (exemple : fichier contenant la CIN est invalide) • **EMAILNOTACCEPTED :** une requête pour (userId, email) est créée et l'adresse email du demandeur du certificat n'est pas acceptée. • **FACETOFACEREQUIRED :** une requête pour (userId, email) est créée et l'identification face à face est exigée. • **GENERATING:** le certificat est en cours de génération. • **GENERATED:** Le certificat a été généré. • **REVOKED :** Le certificat de l'utilisateur est révoqué. • **EXPIRED :** Le certificat de l'utilisateur est expiré.
message	OBLIGATOIRE	String	Selon la valeur du champ **requestStatus**, ce champ contient les valeurs suivantes : • **requestStatus=ONGOING :message=**The request is waiting for validation. • **requestStatus=REJECTED** : **message=** Failure to create digigo user. • **requestStatus= VALID : message=**The request is validated by TunTrust operator. • **requestStatus=MISSING_INFO**: **message=**The request is missing a file. • **requestStatus=FACETOFACEREQUIRED : message=**A face to face identification is required. • **requestStatus=EMAILNOTACCEPTED : message=The email address of subcriber is not accepted by TunTrust.** • **requestStatus=GENERATING:message=**The certificate is issuance is in progress. • **requestStatus=GENERATED:message=**The certificate is issued. • **requesStatus=REVOKED :message=**The certificate is revoked. • **requestStatus=EXPIRED :message=**The certificate is expired.
verificationTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de la vérification de l'état de l'utilisateur.

Error Codes:

Error case	Status Code	Error	Error Description
Le paramètre **clientId** est vide	400 (bad Request)	invalid_request	Missing parameter **clientId**
Le paramètre **clientId** est invalide	400 (bad Request)	invalid_request	Invalid parameter **clientId**
Le paramètre **idType** est invalide	400 (bad Request)	Invalid_request	The parameter **idType** is malformed.
Le paramètre **idType** est vide	400 (bad Request)	Invalid_request	The parameter **idType** is mandatory.
Le paramètre **userId** est invalide	400 (bad Request)	Invalid_request	The parameter **userId** is malformed.
Le paramètre **userId** est vide	400 (bad Request)	Invalid_request	The parameter **userId** is mandatory.

Error case	Status Code	Error	Error Description
Le paramètre **email** est invalide	400 (bad Request)	Invalid_request	The parameter **email** is malformed.
Le paramètre **email** est vide	400 (bad Request)	Invalid_request	The parameter **email** is mandatory.
Erreur interne	500	Internal error	The server encounters an unexpected condition.

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-user-status/694b650c-eceb-4765-94f7-d170b4a1247c/99999999/CIN/foulen@certification.tn HTTP/1.1
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{   "requestSatus": "GENERATED",
    "clientId": "694b650c-eceb-4765-94f7-d170b4a9807a",
    "requestId": "9e376d12-33e3-42d3-a469-5abbd0083132",
    "message" : "The certificate is issued",
    "verificationTimestamp" : 1583486466000
}
```

2.3.8 update-digigo-user/{clientId}/{certType}/{txIdEmail}/{subscriberEmail}

Ce web-service est utilisé par l'AED pour mettre à jour le champ email du demandeur du certificat. Ce service ne peut être appelé qu'après avoir validé l'OTP du nouvel email du demandeur de certificat.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/update-digigo-user/{clientId}/{certType}/{txIdEmail}/{subscriberEmail}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant associé à l'AED.
certType	OBLIGATOIRE (URL)	String	Ce paramètre contient l'une des valeurs suivantes : • **PERSO** : personne physique sans attributs professionnels • **PRO :** personne physique avec des attributs professionnels • **SEAL :** personne morale (cachet électronique)
txIdEmail	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP du nouveau email.
subscriberEmail	OBLIGATOIRE (URL)	String (syntaxe email)	Ce paramètre contient l'adresse email à rectifier du demandeur du certificat pour les certificats PERSO, PRO **(certType=PERSO /PRO)** et contient le prénom du responsable cachet en cas de certificat SEAL **(certType= SEAL).**

Output :

Paramètre	Présence	Valeur	Description

requestId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la requête émise par le client.
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'**AED**.
userId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'utilisateur de l'application de l'AED.
requestStatus	OBLIGATOIRE	String	Ce paramètre contient l'état de la transaction défini comme suit : • **FAILURE** : la mise à jour de l'adresse email a échoué. • **SUCCESS** : la mise à jour de l'adresse email a été effectuée avec succès.
requestTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de l'enregistrement de la requête.

Error Codes :

Type d'erreur	Code d'erreur	Message d'erreur
Le paramètre **clientId** est invalide	400 (bad Request)	The parameter **clientId** is invalid.
Le paramètre **certType** est invalide	400 (bad Request)	The parameter **certType** is malformed.
Le paramètre **txIdEmail** est invalide	400 (bad Request)	The parameter **txIdEmai**l is malformed.
Le paramètre **subscriberEmail** est invalide	400 (bad Request)	The parameter **subscriberEmail** is malformed.
L'adresse **email** du demandeur du certificat est déjà enregistrée	403	The email address ****** is already registred.
Les **OTPs** envoyés ne sont pas encore validés par le demandeur du certificat.	401	The OTPs are not validated by the subscriber.
Erreur interne	500	The server encounters an unexpected condition.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/update-digigo-user/694b650c-eceb-4765-94f7-d170b4a1247c/PRO/5460a4b6-7b1a-47dd-8be5-dbc5c98a4279/flen@certification.tn
Host: digigo.tuntrust.tn
Content-Type: application/json
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
"requestId" : "7742a7d7-8575-44a2-954a-e8c04f0013e1",
"clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
"userId " : "99999999",

"requestStatus" : "SUCCESS",
"requestTimestamp" : 1579594591268
}
```

2.3.9 revoke-certificate/{clientId}

Ce web-service permet la révocation d'un certificat d'un utilisateur. Pour l'authentification de la demande de révocation au moins un OTP de validation est envoyé au porteur du certificat :

- Un SMS OTP est envoyé au numéro de téléphone associé au CIN/Passeport ou carte séjour du porteur du certificat, ou
- Un email OTP est envoyé à une adresse email associée au CIN/Passeport ou carte séjour du porteur du certificat. Au cas où plusieurs certificats sont associés au même porteur, l'adresse email utilisée pour la validation OTP peut ne pas correspondre à l'adresse email associée au certificat à révoquer.

Input :
https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/revoke-certificate/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
email	OBLIGATOIRE	String	Ce paramètre correspond à l'adresse email du porteur du certificat.
idType	OBLIGATOIRE	String	Il permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR** •
txIdPhone	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP de type SMS. **Le numéro de téléphone doit être associé au userId.**
txIdEmail	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP de type EMAIL. L'adresse email doit être associée au **userId**. Si l'utilisateur possède plusieurs certificats avec le même **userId** mais des adresses emails différentes, l'adresse email utilisée pour la validation de l'OTP peut ne pas correspondre à l'adresse email du certificat à révoquer.
revocationReason	OBLIGATOIRE	String	Ce paramètre contient la raison de la révocation. Ce paramètre contient l'une des valeurs suivantes : **- KEY_COMPROMISE :** la clé privée est compromise (perte de téléphone, perte d'accès à la boite de messagerie électronique, perte code PIN du certificat) **- CESSATION_OF_OPERATION :** l'entité associée au certificat a arrêté ses opérations ou bien le titulaire de certificat (individu ou organisation) cessant ses activités concernées. **- SUPERSEDED :** signifie que le certificat a été remplacé par un nouveau : Un certificat précédent n'est plus valide en raison de mises à niveau, de modifications de stratégie ou de renouvellement de clé.

- **AFFILIATION_CHANGED :** la propriété, la gestion ou la structure organisationnelle de l'entité associé au certificat a changé.

- **- UNSPECIFIED :** le demandeur n'a pas spécifié la raison de la révocation de son certificat.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'AED.
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de traitement de la révocation et contient l'une des valeurs suivantes : • **SUCCESS (code : 202)** : la demande de révocation authentifiée et effectuée avec succès. • **FAILURE** : la demande de révocation de certificat a échoué.

Error Codes :

Cas erreur	status	erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is invalid.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **txIdPhone** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **txIdPhone** is invalid. Le numéro de téléphone n'est pas associé au **userId**.
Le paramètre **txIdEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **txIdEmail** is invalid. L'adresse email n'est pas associée au **userId**.
Aucun certificat valide pour (userId, email)	NOT FOUND	404	Not found valid certificate for (userId, email)
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/revoke-certificate/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"userId" : "99999999",
"idType" : " CIN ",
“email”: “foulen@certification.tn”,
```

```
"txIdPhone": "16a1713f-2954-4720-b271-a90ce6dad84a",
"txIdEmail": "b180a48b-affd-4e99-9c8a-b61ad7949b23",
"revocationReason": "CLE_COMPROMISE"
}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/revoke-certificate
Content-Type: application/json
{
"clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
"userId" : "99999999",
"status" : "SUCCESS"
}
```

2.3.10 unlock-pin/{clientId}

Ce web-service permet le déverrouillage d'd'un certificat Digigo bloqué suite à 03 tentatives erronées de connexion.

La demande de déblocage du code PIN doit être authentifiée à travers l'envoi du code OTP sur le numéro de téléphone portable ou à l'adresse email associé au certificat à débloquer.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/unlock-pin/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
email	OBLIGATOIRE	String	Ce paramètre correspond à l'adresse email du porteur du certificat.
idType	OBLIGATOIRE	String	Il permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
authDelivery	OBLIGATOIRE	Int	Ce paramètre indique le moyen de communication utilisé pour envoyer l'OTP : **1 = SMS** **2 = EMAIL**
txIdPhone	OBLIGATOIRE conditionnel	String	Ce paramètre indique le moyen de la transaction relative à l'envoi OTP de type SMS. Le numéro de téléphone utilisé pour la validation du SMS OTP doit être associé au userId. Ce champ est obligatoire si **authDelivery =1.**
txIdEmail	OBLIGATOIRE conditionnel	String	Ce paramètre correspond à l'identifiant de la transaction relative à l'envoi OTP de type email. L'adresse email utilisée pour la validation OTP doit être identique à l'adresse email du certificat à débloquer. Ce champ est obligatoire si **authDelivery =2.**

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'AED.

userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de traitement de la demande de déblocage du code PIN: • **SUCCESS (code : 200)** : le déblocage est effectué avec succès. • **FAILURE** : le déblocage a échoué.

Erreur Codes :

Cas erreur	Status	erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is invalid.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **txIdPhone** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **txIdPhone** is invalid.
Le paramètre **txIdEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **txIdEmail** is invalid.
Le paramètre **txIdEmail** est vide si **authDelivery=2**	INVALID REQUEST	400 (bad Request)	The parameter **txIdEmail** is mandatory.
Le paramètre txIdPhone est vide si **authDelivery=1**	INVALID REQUEST	400 (bad Request)	The parameter **txIdPhone** is mandatory.
Aucun certificat valide pour (userId, email)	NOT FOUND	404	Not found valid certificate for (userId, email)
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/unlock-pin/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"userId" : "99999999",
"idType" : " CIN ",
“email": "foulen@certification.tn",
"authDelivery" : 1,
"txIdPhone" : "f455c39c-5be3-427a-8e10-f84e80f53c35"}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/unlock-pin
Content-Type: application/json
{
"clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
"userId" : "99999999",
"status" : "SUCCESS"}
```

2.3.11 request-affiliation/{clientId}

Ce web-service permet d'associer un nouveau matricule fiscal à un utilisateur existant ayant un certificat DigiGO valide (non expiré et non révoqué). Trois types d'affiliation peuvent associer un utilisateur à une organisation :

- Affiliation représentant légal indiqué dans le RNE ou le registre de commerce pour les pays étrangers.
- Affiliation collaborateur pour associer un employé à une organisation .
- Affiliation administrateur pour désigner un utilisateur ayant des privilèges octroyés par le représentant légal pour affilier d'autres utilisateurs à son organisation.

Ajout d'un représentant légal à une organisation :

- L'utilisateur souhaitant ajouter une affiliation de type représentant légal d'une organisation doit initialement avoir un certificat DIGIGO.
- La requête d'ajout d'une affiliation de type représentant légal à une organisation doit être signée par l'utilisateur dont le CIN/ le passeport ou carte de séjour correspond à l'identifiant du représentant légal listé dans le RNE ou sur le registre de commerce pour les organisations étrangères.

Ajout d'un collaborateur à une organisation :

- L'affiliation d'un collaborateur à une organisation ne peut se faire que par le représentant légal ou l'administrateur de l'organisation. Dans ce cas, le représentant légal ou l'administrateur doit initialement avoir un certificat DIGIGO associé à cette organisation.
- La requête d'ajout d'une affiliation de type collaborateur à une organisation doit être signée par le représentant légal ou l'administrateur de l'organisation.
- Un lien d'approbation de cette demande d'affiliation est par la suite transmis au collaborateur pour apposer sa signature en guise de consentement.

Ajout d'un administrateur à une organisation :

- L'affiliation d'un administrateur à une organisation ne peut se faire que par le représentant légal ou l'administrateur de l'organisation. Dans ce cas, le représentant légal ou l'administrateur doit initialement avoir un certificat DIGIGO associé à cette organisation.
- Une organisation peut au plus avoir deux administrateurs.
- La requête d'ajout d'une affiliation de type administrateur à une organisation doit être signée par le représentant légal ou un autre administrateur de l'organisation.
- Un lien d'approbation de cette demande d'affiliation administrateur est par la suite transmis au concerné pour apposer sa signature en guise de consentement.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/request-affiliation/{clientId}

Paramètre	Présence	Valeur	Description

clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
idType	OBLIGATOIRE	String	Il permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
email	OBLIGATOIRE	String	Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.
affiliationType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type d'affiliation du porteur du certificat par rapport à l'organisation : • **LEGALREP** • **COLLABO** • **ADMIN**
requestorIdType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
requestorId	OBLIGATOIRE	String	Ce paramètre **requestorId** contient le numéro CIN/ passeport/carte de séjour du représentant légal ou de l'administrateur de l'organisation
requestorEmail	OBLIGATOIRE	String	Ce paramètre **requestorEmail** contient l'adresse email associée au compte Digigo du représentant légal ou de l'administrateur de l'organisation
requestSignature	OBLIGATOIRE	String/base64	Ce paramètre contient la signature par le certificat associé au (requestorId, requestorEmail) de tous les champs de cette transaction.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant associé à l'**AED initiale**.
affiliationRqtId	OBLIGATOIRE	String	Identifiant unique de la requête d'affiliation attribué par TunTrust
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
affiliationRqtStatus	OBLIGATOIRE	String	Ce paramètre contient l'une des valeurs suivantes : • **SUCCESS :** la requête d'affiliation a été traitée (cas ou le demandeur est lui-même un représentant légal ou bien un administrateur de l'organisation) • **PENDING** (code 202) : la requête est en attente de validation. • **REJECTED** : en cas d'échec de création de l'utilisateur

affiliationRqtTimestamp	OBLIGATOIRE	Timestamp	Ce paramètre correspond à la date et heure de l'enregistrement de la requête sous format **[UTC time mill sec UNIX]**.

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **organisationId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** est introuvable	INVALID REQUEST	404	The parameter **organisationId** is not found.
Le représentant légal n'est pas autorisé à effectuer cette transaction.	INVALID REQUEST	404	The legal representative is not allowed to perform this transaction.
Le paramètre **affiliationType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **affiliationType** is malformed.
Le paramètre **affiliationType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **affiliationType** is mandatory.
Le paramètre **requestorIdType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is malformed.
Le paramètre **requestorIdType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is mandatory.
Le paramètre **requestorId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is malformed.
Le paramètre **requestorId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is mandatory.
Le paramètre **requestorEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is malformed.
Le paramètre **requestorEmail** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is mandatory.
Le paramètre **requestSignature** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is invalid.
Le paramètre **requestSignature** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is mandatory.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/request-affiliation/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"userId" : "99999999",
"idType" : " CIN ",
"email": "foulen@certification.tn",
"organisationId": "1111111A",
"affiliationType": “COLLABO",
"requestorIdType":"CIN",
"requestorId":"99999988",
"requestorEmail": "flen@certification.tn",
"requestSignature ": "+PGRzOlNpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDo…"}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
"affiliationRqtId":"9217b17f-f1df-4fe2-9d2e-1d98662e0365",
"clientid": "694b650c-eceb-4765-94f7-d170b4a1247c",
"userId" : "99999999",
"affiliationRqtStatus" : "PENDING",
“affiliationRqtTimestamp”: “1583486466000”
}
```

2.3.12 approve-affiliation /{clientId}

Ce web-service permet à un collaborateur ou un administrateur d’approuver la demande d’affiliation d’une organisation à son certificat DIGIGO.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/approve-affiliation/{clientId}

Paramètre	Présence	Valeur	Description
affiliationRqtId	OBLIGATOIRE	String	Identifiant unique de la requête d’affiliation attribué par TunTrust
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l’identifiant de l’AED.
idType	OBLIGATOIRE	String	Ce paramètre permet d’identifier le type de pièce d’identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
email	OBLIGATOIRE	String	Ce paramètre correspond à l’adresse email correspondante au certificat à affilier à l’organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l’identifiant de l’organisation à dissocier. Si le champ **country est TN**, ce paramètre contient l’identifiant RNE de l’organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du

			format.
affiliationType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type d'affiliation du porteur du certificat par rapport à l'organisation : • **LEGALREP** • **COLLABO** • **ADMIN**
RequestorIdType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
requestorId	OBLIGATOIRE	String	Ce paramètre **requestorId** contient le numéro CIN/passeport /carte de séjour du représentant légal ou de l'administrateur de l'organisation
requestorEmail	OBLIGATOIRE	String	Ce paramètre **requestorEmail** contient l'adresse email associée au compte Digigo du représentant légal ou de l'administrateur de l'organisation
approvalSignature	OBLIGATOIRE	String/base64	Ce paramètre contient la signature par le certificat associé au collaborateur ou l'administrateur à associer à l'organisation

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.
affiliationRqtId	OBLIGATOIRE	String	Identifiant unique de la requête d'affiliation attribué par TunTrust.
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
affiliationRqtStatus	OBLIGATOIRE	String	Ce paramètre contient l'état de traitement d'ajout du matricule fiscal : • **SUCCESS (code : 200)** : le matricule fiscal est associé avec succès. • **FAILURE :** l'ajout du matricule fiscal a échoué.
affiliationRqtTimestamp	OBLIGATOIRE		Ce paramètre correspond à la date et heure de l'enregistrement de la requête sous format [UTC time mill sec UNIX].

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **affiliationRqtId** est invalide.	INVALID REQUEST	400 (bad Request)	The **affiliationRqtId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID	400 (bad Request)	The parameter **userId** is mandatory.

	REQUEST		
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter email is malformed.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **organisationId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** est introuvable	INVALID REQUEST	404	The parameter **organisationId** is not found.
Le représentant légal n'est pas autorisé à effectuer cette transaction.	INVALID REQUEST	404	The legal representative is not allowed to perform this transaction.
Le paramètre **affiliationType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **affiliationType** is malformed.
Le paramètre **affiliationType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **affiliationType** is mandatory.
Le paramètre **requestorIdType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is malformed.
Le paramètre **requestorIdType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is mandatory.
Le paramètre **requestorId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is malformed.
Le paramètre **requestorId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is mandatory.
Le paramètre **requestorEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is malformed.
Le paramètre **requestorEmail** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is mandatory.
Le paramètre **approvalSignature** est vide	INVALID REQUEST	400 (bad Request)	The parameter **approvalSignature** is mandatory.
Le paramètre **approvalSignature** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **approvalSignature** is invalid.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/approve-affiliation/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"affiliationRqtId" : "9217b17f-f1df-4fe2-9d2e-1d98662e0365",
"userId" : "99999999",
"idType" : " CIN ",
"email": "foulen@certification.tn",
"organisationId ": "1111111A",
“affiliationType”: “COLLABO",
“requestorIdType”:”CIN”,
“requestorId”:”99999988”,
“requestorEmail”: “flen@certification.tn”,
“approvalSignature”: “+iojekjjsqodoiuieruepzrueuriezuri…”
}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
   "affiliationRqtId" : "9217b17f-f1df-4fe2-9d2e-1d98662e0365",
   "clientId" : "694b650c-eceb-4765-94f7-d170b4a1247c",
   "userId" : "99999999",
   "affiliationRqtStatus" : "SUCCESS",
   "affiliationRqtTimestamp" : 1593683840704
}
```

2.3.13 get-affiliation/{clientId}/{affiliationRqtId}

Ce web service permet à une AED de vérifier une demande d'affiliation déjà créé et activée.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-affiliation/{clientId}/{affiliationRqtId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
affiliationRqtId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant unique de la requête d'affiliation attribué par TunTrust.

Output :

Paramètre	Présence	Valeur	Description
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro CIN/ passeport/carte de séjour.
idType	OPTIONAL	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
email	OBLIGATOIRE	String	Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'organisation à dissocier. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.
Organisation	OBLIGATOIRE Conditionnel	String <= 200 caractères	Ce paramètre correspond à la raison sociale de l'organisation. Ce champ est obligatoire uniquement dans le cas de certificats de type **PRO et SEAL.**
affiliationType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type d'affiliation du porteur du certificat par rapport à l'organisation :

			• **LEGALREP** • **COLLABO** • **ADMIN**
RequestorIdType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
requestorId	OBLIGATOIRE	String	Ce paramètre **requestorId** contient le numéro de la CIN/du passeport /de la carte de séjour du représentant légal ou de l'administrateur de l'organisation.
requestorEmail	OBLIGATOIRE	String	Ce paramètre **requestorEmail** contient l'adresse email associée au compte Digigo du représentant légal ou de l'administrateur de l'organisation.
requestSignature	OBLIGATOIRE	String/base64	Ce paramètre contient la signature par le certificat associé au {requestorId, requestorEmail} de tous les champs de cette transaction.

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **affiliationRqtId** est invalide.	INVALID REQUEST	400 (bad Request)	The **affiliationRqtId** is invalid.
Le paramètre **affiliationRqtId** est vide.	INVALID REQUEST	400 (bad Request)	The **affiliationRqtId** is mandatory

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-affiliation/694b650c-eceb-4765-94f7-d170b4a1247c/893e60d0-5a3f-44b3-9701-e40ad9867087

Host: digigo.tuntrust.tn

Content-Type: application/json
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-affiliation
Content-Type: application/json
{
"idType": CIN,

"userId": 09090909,

    "email": foulen@certification.tn,

    "organisationId": "1111111X",

    "organisation": "XXXXX ",

    "affiliationType": "COLLABO",
```

```
    "requestorIdType": "CIN",

    "requestorId": "00222222",

    "requestorEmail": "responsable@certification.tn",

    "requestSignature": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5v
Ij8+PGRzOlNpZ25hdHVyZSB4b..." }
```


2.3.14 aed-user-info/{clientId}/{email}

Ce web-service permet de récupérer l'affiliation associée à un utilisateur ayant un certificat DigiGo.

Input:

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-user-info/{clientId}/{email}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
idType	OPTIONAL	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
userId	OPTIONAL	String	Ce paramètre **userId** contient le numéro de la CIN/ du passeport/ de la carte de séjour.
email	OBLIGATOIRE (URL)		Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OPTIONAL	String	Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.
email	OBLIGATOIRE	String	Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.

affiliationType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type d'affiliation du porteur du certificat par rapport à l'organisation : • **LEGALREP** • **COLLABO** • **ADMIN**

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **organisationId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** est introuvable	INVALID REQUEST	404	The parameter **organisationId** is not found.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/aed-user-info/694b650c-eceb-4765-94f7-d170b4a1247c/foulen@certification.tn
Host: digigo.tuntrust.tn
Content-Type: application/json
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
"clientId":"694b650c-eceb-4765-94f7-d170b4a1247c"
" email": "foulen@certification.tn",
"organisations":[
    {
    "organisationId ": "1111111A",
    "affiliationType": "COLLABO"
    }
  ]
}
```

2.3.15 cancel-affiliation/{clientId}

Ce web-service permet de supprimer l'affiliation associée à un utilisateur.

Input:

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/cancel-affiliation/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
idType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
userId	OBLIGATOIRE Conditionnel	String	Ce paramètre **userId** contient le numéro de la CIN/ du passeport/de la carte de séjour.
email	OBLIGATOIRE		Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.
RequestorIdType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
requestorId	OBLIGATOIRE	String	Ce paramètre **requestorId** contient le numéro de la CIN/du passeport /de la carte de séjour du représentant légal ou de l'administrateur de l'organisation.
requestorEmail	OBLIGATOIRE	String	Ce paramètre **requestorEmail** contient l'adresse email associée au compte Digigo du représentant légal ou de l'administrateur de l'organisation.
requestSignature	OBLIGATOIRE	String/base64	Ce paramètre contient la signature par le certificat associé au {requestorId, requestorEmail} de tous les champs de cette transaction.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de traitement de la suppression d'affiliation: • **SUCCESS (code : 200)** : l'affiliation a été supprimée avec succès • **FAILURE :** la suppression du matricule fiscal a échoué.

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est	INVALID	400 (bad Request)	The **clientId** is invalid.

invalide.	REQUEST		
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **organisationId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** est introuvable	INVALID REQUEST	404	The parameter **organisationId** is not found.
Le représentant légal n'est pas autorisé à effectuer cette transaction.	INVALID REQUEST	404	The legal representative is not allowed to perform this transaction.
Le paramètre **requestorIdType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is malformed.
Le paramètre **requestorIdType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is mandatory.
Le paramètre **requestorId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is malformed.
Le paramètre **requestorId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is mandatory.
Le paramètre **requestorEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is malformed.
Le paramètre **requestorEmail** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is mandatory.
Le paramètre **requestSignature** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is invalid.
Le paramètre **requestSignature** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is mandatory.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/cancel-affiliation/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"userId" : "99999999",
"idType" : " CIN ",
"email": "foulen@certification.tn",
"organisationId ": "1111111A",
"requestorIdType":"CIN ",
"requestorId":"99999988",
"requestorEmail": "flen@certification.tn ",
"requestSignature ": "PGRzOlNpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDo…"
}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/cancel-affiliation
Content-Type: application/json
{
"clientId":"694b650c-eceb-4765-94f7-d170b4a1247c",
"Status" : "SUCCESS"
}
```

2.3.16 change-affiliation/{clientId}

Ce web-service permet de changer l'affiliation d'un utilisateur.

Input:

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/change-affiliation/{clientId}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
idType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
userId	OBLIGATOIRE	String	Ce paramètre **userId** contient le numéro de la CIN/ du passeport/ de la carte de séjour.
email	OBLIGATOIRE		Ce paramètre correspond à l'adresse email correspondante au certificat à affilier à l'organisation.
organisationId	OBLIGATOIRE	String	Ce paramètre contient l'identifiant de l'organisation. Si le champ **country est TN**, ce paramètre contient l'identifiant RNE de l'organisation (7 chiffres et une lettre). Il est validé par un algorithme de vérification du format.
affiliationType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type d'affiliation du porteur du certificat par rapport à l'organisation : • **LEGALREP** • **COLLABO** • **ADMIN**
RequestorIdType	OBLIGATOIRE	String	Ce paramètre permet d'identifier le type de pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**
requestorId	OBLIGATOIRE		Ce paramètre **requestorId** contient le numéro de la CIN / du passeport / de la carte de séjour du représentant légal ou de l'administrateur de l'organisation
requestorEmail	OBLIGATOIRE		Ce paramètre **requestorEmail** contient l'adresse email associée au compte Digigo du représentant légal ou de l'administrateur de l'organisation.
requestSignature	OBLIGATOIRE	String/base64	Ce paramètre contient la signature par le certificat associé au {requestorId, requestorEmail} de tous les

Paramètre	Présence	Valeur	Description
			champs de cette transaction.

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.
status	OBLIGATOIRE	String	Ce paramètre contient l'état de traitement du changement d'affiliation : • **SUCCESS (code : 200)** : Le changement de l'affiliation a été effectué avec succès. • **FAILURE** : Le changement a échoué.

Error Codes :

Cas erreur	Status	Erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide.	INVALID REQUEST	400 (bad Request)	The **userId** is invalid.
Le paramètre **userId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **userId** is mandatory.
Le paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is invalid.
Le paramètre **idType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is mandatory.
Le paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
Le paramètre **email** est vide	INVALID REQUEST	400 (bad Request)	The parameter **email** is mandatory.
Le paramètre **organisationId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **organisationId** is malformed.
Le paramètre **organisationId** est introuvable	INVALID REQUEST	404	The parameter **organisationId** is not found.
Le paramètre **affiliationType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **affiliationType** is malformed.
Le paramètre **requestorIdType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is malformed.
Le paramètre **requestorIdType** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorIdType** is mandatory.
Le paramètre **requestorId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is malformed.
Le paramètre **requestorId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorId** is mandatory.
Le paramètre **requestorEmail** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is malformed.
Le paramètre **requestorEmail** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestorEmail** is mandatory.
Le paramètre **requestSignature** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is invalid.
Le paramètre **requestSignature** est vide	INVALID REQUEST	400 (bad Request)	The parameter **requestSignature** is mandatory.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected

condition

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/change-affiliation/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
{
 "userId" : "99999999",
 "idType" : " CIN ",
 " email": " foulen@certification.tn",
 "organisationId ": "1111111A",
 "affiliationType": "COLLABO":
 " requestorIdType":"CIN ",
 " requestorId”: "99999988",
 " requestorEmail": "flen@certification.tn ",
 "requestSignature ": "+PGRzOlNpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDo…" }
```

Exemple de réponse :

```
HTTP/1.1 200 Found
Location: https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/change-affiliation
Content-Type: application/json
{
"clientId": "694b650c-eceb-4765-94f7-d170b4a1247c",
"status" : "SUCCESS"
}
```

2.3.17 get-quota/{clientId}

Ce web-service est utilisé pour connaître le quota associé à une AED , ou bien pour récupérer le quota d'un utilisateur final.

Input :

- **AED :** https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-quota/{clientId}
- **USER :** https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-quota/{clientId}/{email}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
email	OBLIGATOIRE conditionnel (URL)	String	Ce paramètre correspond à l'adresse email correspondante à l'utilisateur à récupérer son quota.
userId	OPTIONAL	String	Ce paramètre **userId** contient le numéro de la CIN/du passeport/de la carte de séjour.
idType	OPTIONAL	String	Il permet d'identifier le type de la pièce d'identité. Ce paramètre contient trois types de valeurs : • **CIN** • **PASSEPORT** • **CARTESEJOUR**

Output :

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.
remain	OBLIGATOIRE	Number	Ce paramètre correspond au quota restant.
dateExpire	OBLIGATOIRE	String	Ce paramètre contient la date d'expiration du quota sous format [UTC time mill sec UNIX].
txId	OBLIGATOIRE	String	Ce paramètre correspond à l'ID du Transaction.
dateOrder	OBLIGATOIRE		Ce paramètre contient la date d'obtention du quota sous format [UTC time mill sec UNIX].
type	OBLIGATOIRE	String	Ce paramètre contient le Type de quota : • SIG : quota de Signature • TST : quota d'horodatage

Error Codes :

Cas erreur	Status	Code	Description
La syntaxe du paramètre **clientId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is malformed.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **userId** est invalide	INVALID REQUEST	400 (bad Request)	Invalid **userId**
userId est introuvable	NOT FOUND	404	**userId** not found
La syntaxe du paramètre **idType** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **idType** is malformed.
La syntaxe du paramètre **email** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **email** is malformed.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-quota/694b650c-eceb-4765-94f7-d170b4a1247c
Host: digigo.tuntrust.tn
Content-Type: application/json
```

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy-admin/get-quota/694b650c-eceb-4765-94f7-d170b4a1247c/foulen@certification.tn
Host: digigo.tuntrust.tn
Content-Type: application/json
{
"userId" : "99999999",
"idType" : "CIN"
}
```

Exemple de réponse :

```
Content-Type: application/json
{
"txId": "1",
"remain": 100,
"dateOrder": 1593117126000,
"dateExpire": 1624653126000,
"type": "SIG"
}
```

3 Signer électroniquement avec DIGIGO

L'API DigiGo permet aux intégrateurs d'effectuer les fonctions d'authentification et de signature à distance suivantes :

Nom du service	Fonction
credentials/info	Récupérer le certificat ou la chaine de certification d'un utilisateur DigiGo.
oauth2/authorize	Permettre à un utilisateur d'utiliser une ressource distante, cette fonction retourne un code d'autorisation, que l'application de signature DOIT ensuite utiliser pour obtenir un jeton d'accès avec la méthode oauth2 /token.
oauth2/token	Associer un jeton (token) d'accès à un utilisateur donné.
signatures/signHash	Calculer la signature numérique à distance d'une ou plusieurs valeurs de hachage fournies en entrée. Cette méthode nécessite une autorisation d'identification sous la forme de données d'activation de signature (sad). L'application de signature doit d'abord passer à cette méthode **sad** obtenu lors de l'appel des web services **oauth/authorize** et **oauth/token**.
credentials/extendTransaction	- Prolonger la validité d'une autorisation de transaction multi-signature en obtenant de nouvelles données d'activation de signature (sad) lorsque la méthode signatures/signHash est invoquée plusieurs fois avec un seul sad. -Renouveler un sad, avant son expiration.
timestamp	Permet de générer un jeton d'horodatage pour la valeur de hachage donnée en entrée.

3.1 credentials/info/{clientId}/{credentialId}/{certificates}

Ce web-service permet de récupérer le certificat d'un utilisateur et sa chaîne de confiance.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/credentials/info/{clientId}/{credentialId}/{certificates}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'identifiant de l'AED.
credentialId	OBLIGATOIRE (URL)	String	Ce paramètre correspond à l'adresse email du porteur du certificat.
certificates	OBLIGATOIRE (URL)	String	Spécifie quels certificats de la chaîne de certificats doivent être retournés. Ce paramètre contient la valeur suivante : «**chain**»: la chaîne de certificats complète DOIT être retournée y compris le certificat du signataire au début.

Output :

Attribute	Presence	Value	Description
cert/certificates	OBLIGATOIRE	*Array of String*	Ce paramètre contient un ou plusieurs certificats encodés en Base64. Pour le paramètre ***certificates* = "chain"**, ce champ retourne la totalité de la chaine de confiance avec le certificat de l'utilisateur final au début.

Error Codes :

Cas erreur	status	erreur	Description
Le paramètre **clientId** est invalide.	INVALID REQUEST	400 (bad Request)	The **clientId** is invalid.
Le paramètre **clientId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **clientId** is mandatory.
Le paramètre **credentialId** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **credentialId** is invalid.
Le paramètre **credentialId** est vide	INVALID REQUEST	400 (bad Request)	The parameter **credentialId** is mandatory.
Le paramètre **certificates** est invalide	INVALID REQUEST	400 (bad Request)	The parameter **certificates** is invalid.
Erreur interne	INTERNAL ERROR	500	The server encounters an unexpected condition

Exemple de requête :

```
GET https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/credentials/info/694b650c-eceb-4765-94f7-d170b4a9807c/foulen@certification.tn/chain
Host: digigo.tuntrust.tn
Content-Type: application/json
```

Exemple de réponse :


```
HTTP/1.1 200 Found
Content-Type: application/json

  "certificates": [

 {"encodedCertificate": "MIIFqjCCBBKgAwIBAgIIVc1AajyHgdMwDQYJKoZIhvcNAQELBQAwZjELMzEzbjxCg/aYOI
Jwzdq/6ODmdhZ0rKJX26r2vJ5OvYbwamNM3Pw0u+whkyFiV8ctQ6NLNP7NO50REcS3TcdI/V8clMYwGPPylbYjiPBoz8mMu
EkQitJRxyHVanXsc/piOhrpFlDNm1lWRvpODM3Bfe90o93/HBWw6hOqCuF7MXMDmDLXsg3dPlbMmNujr+rIsHwFo94AU="}
,

{"encodedCertificate": "MIIFqjCCBBKgAwIBAgIIVc1AajyHgdMwDQYJKoZIhvcNAQELBQAwZjELMzEzbjxCg/aYOIJ
wzdq/6ODmdhZ0rKJX26r2vJ5OvYbwamNM3Pw0u+whkyFiV8ctQ6NLNP7NO50REcS3TcdI/V8clMYwGPPylbYjiPBoz8mMuE
kQitJRxyHVanXsc/piOhrpFlDNm1lWRvpODM3Bfe90o93/HBWw6hOqCuF7MXMDmDLXsg3dPlbMmNujr+rIsHwFo94AU="},

        {
"encodedCertificate": "MIIF8zCCA9ugAwIBAgIINnFvpDbswtIwDQYJKoZIhvcNAQELBQAwZjELMAkGA1UEBhMCVE4x
DjAMBgNVBAcMBVR1bmlzMS4wLAYDVQQKDCVOYXRpb25hbCBEaWdpdGFsIENlcnRpZmljYXRpb24gQWdlbmN5MRcwFQYDVQQ
DDA5UdW5pc2lhIEdvdiBDQTAeFw0xNjExMjkxMDQ3MDFaFw0yNjEyMjkxMDQ3MDFaMGYxCzAJBgNVBAYTAlROMQyQiOImSA
58CVhZqFd0tglFCKjmwUiShSTfIvbLPGXdJbfyBGK7YQDFI"},

        {"encodedCertificate": "MIIGdzCCBF+gAwIBAgIIeCwQCYMKS+4wDQYJKoZIhvcNAQELBQAwcDELMAkGA1U
EBhMCVE4xDjAMBgNVBAcMBVR1bmlzMS4wLAYDVQQKDCVOYXRpb25hb5T75YTx0Y4mnFkyL5mr5imjgqX/DBa9QiWf908dIR
TlTomS3PfChzJLt3hIZUyp7sgRJfZyw4PRjDRL8CAwEAAaOCAR0wggEZMDYGCCsGAQUFBwEBBCowKDAmBggrBgEFBQcwAYY
aaHR0cDovL3ZhLmNlcnRpZmlj18NJHsbEXajLijzvCLpxAWYYj"},

        {
"encodedCertificate": "MIIGuO2JSxSAsPsFynrEhd6nIUoln3d0lZXWBCXj8Y7y/vnDAf/v/gKH7/fqPI89aLAi4p7c
qFDxgHHWBFBaLiSf1IkIIIgx3a+74YrC1RsR4+8RSSX8xaGW8AO435V8+ENNlgLox/Q/JXoSXV9psppCoP+y5Ei1ra5hPG9
4+zWEEkPa8Okn+a3oRCKrXbzMFVffOjJEjEgBkW4wXhnhMCmHC1UJE9ZibdNTkc=" }

]
```


→ Le premier **"encodedCertificate"** est le certificat du signataire, ceux qui suivent sont les certificats des autorités qui l'ont émise (chaine de certification).

3.2 oauth2/authorize

Pour permettre à un utilisateur d'utiliser une ressource distante, la fonction oauth2/authorize retourne un token d'autorisation (token jwt) que l'application de signature DOIT ensuite utiliser pour obtenir un jeton d'accès avec la méthode oauth2 /token (sad).

À la fin du processus d'autorisation, le serveur d'autorisation DEVRA rediriger l'utilisateur vers l'URI spécifiée par le paramètre redirectUri pré-enregistré auparavant chez Tuntrust.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/oauth2/authorize?redirectUri=https%3A%2F%2Flocalhost%3A8443%2Fprotected-resource&responseType=code&scope=credential&credentialId= folen.benfoulen@certification.tn &clientId=694b650c-eceb-4765-94f7-d170b4a9807c&numSignatures=1&hash=LPJNul%2Bwow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ%3D

Paramètre	Présence	Valeur	Description
responseType	OBLIGATOIRE (URL)	String	Cette valeur doit être égale à « code ».
clientId	OBLIGATOIRE	String	Ce paramètre correspond à l'identifiant de l'AED.

Paramètre	Présence	Valeur	Description
	(URL)		
redirectUri	OBLIGATOIRE (URL)	String	L'URL où l'utilisateur sera redirigé après que le processus d'autorisation est terminé. Seul un URI valide, pré-enregistrée chez le serveur d'autorisation Digigo, doit être transmise. Ce paramètre est **UrlEncoded**.
scope	OBLIGATOIRE (URL)	String	Ce paramètre contient la valeur « credential »
credentialId	OBLIGATOIRE (URL)	String	Email du signataire
numSignatures	OBLIGATOIRE CONDITIONNEL (URL)	Number	Ce paramètre contient le nombre de signatures à autoriser. Les transactions multi-signatures peuvent être obtenues en utilisant une combinaison de tableau de valeurs d'empreintes (hash) et en appelant plusieurs fois la méthode **signatures/signHash**.
hash	OBLIGATOIRE CONDITIONNEL (URL)	string	Ce paramètre contient une ou plusieurs valeurs de hachage codées en base64. Il permet au serveur de lier le **sad** à l'empreinte (hash), empêchant ainsi une autorisation à être utilisée pour signer un contenu différent. Plusieurs valeurs d'empreintes (hash) peuvent être transmises en tant que valeurs séparées par des virgules. L'ordre des valeurs multiples ne doit pas nécessairement correspondre à l'ordre des empreintes transmises à la méthode **signatures/signHash.** **Ce paramètre doit être UrlEncoded.**

Output :

Attribute	Presence	Value	Description
token	OBLIGATOIRE	String	Ce paramètre correspond au token d'autorisation (un token jwt). Il DOIT être lié à l'identifiant du client et à l'URI de redirection. Il DOIT expirer peu de temps après sa publication pour atténuer le risque de fuites (5 minutes). L'application de signature ne peut pas utiliser la valeur plusieurs fois. Le paramètre code à utiliser dans oauth2/token est dans la balise **jti** du token d'autorisation. Ce token est signé par le serveur d'autorisation.

Error Codes :

Error case	Status Code	Error	Error Description
Le paramètre "**responseType**" est vide	400 (bad Request) (bad request)	invalid_request	Missing parameter **responseType**
Le paramètre " **responseType** " est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **responseType**
Le paramètre "**clientId**" est vide	400 (bad Request) (bad request)	invalid_request	Missing parameter **clientId**
Le paramètre "**clientId**" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **clientId**
Le paramètre "**redirectUri**" est vide	400 (bad Request) (bad request)	invalid_request	parameter **redirectUri** is not present

Error case	Status Code	Error	Error Description
Le paramètre "**redirectUri**" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **redirectUri**
Le paramètre "**scope**" est vide	400 (bad Request) (bad request)	invalid_request	Missing parameter **scope**
Le paramètre " **scope** " est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **scope**
Le paramètre "**credentialId**" est vide	400 (bad Request) (bad request)	invalid_request	Missing parameter **credentialId**
Le paramètre " **credentialId** "est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **credentialId**
Le paramètre "**numSignatures**" est vide	400 (bad Request) (bad request)	invalid_request	Missing parameter **numSignatures**
Le paramètre " **numSignatures**" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **numSignatures**
Le paramètre "**hash**" est vide	400 (bad Request) (bad request)	invalid_request	Empty hash array
Le paramètre "**hash**" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid Base64 hash string parameter

Exemple de requête :

```
https://digigo.tuntrust.tn/tunsign-proxy-webapp/oauth2/authorize?redirectUri=https%3A%2F%2Flocalhost%3A8443%2Fprotected-resource&responseType=code&scope=credential&credentialId=folen.benfoulen@certification.tn&clientId=694b650c-eceb-4765-94f7-d170b4a9807c&numSignatures=1&hash=LPJNul%2Bwow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ%3D
```

Exemple de réponse :

```
https://localhost:8443/protected-resource?token=eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJtZXJpZW0uemll0b3VuaUBjZXJ0aWZpY2F0aW9uLnRuIiwiaXNzIjoiRGlnaWdvIiwianRpIjoiNmFjYjY1ZDEtNDQ3Ni00ZjJiLTlhYmYtZjYwNGJjZGQ5YzgxIiwiaWF0IjoxNTg3MTY5NTI1LCJleHAiOjE1ODcxNzA0MjUsImF6cCI6IjY5NGI2NTBjLWVjZWItNDc2NS05NGY3LWQxNzBiNGE5ODA3YSJ9.beFBbzbBOH5SV1i2jmdQtJkqELl_K-LSTHAvBRsDefz4s3w53gUi8Nwx-8QFHfZUQs_2DAlLA9NUqIkaNjZ-s572kF-EkaR4AMIRQeJJY7WcoH0m-sPiqyOhFnTMfpmAWPx-2ymC2nISGMcR62KDZUyuSGDB3gFo1ktzgG3rXf30driDqd3Z7M4OCIWzqfLp01k2bjwCF2sOy58eEHKQEYpQyu6ewcfc_UvzroXdwkmosNvG4Xb8pECq7h6aAL3n--lDIvlHWufN1cyj7DFZwaRuN4HX5H94wt5DjexICnk8705nh3g-DiRRqhUA6og1gcbH5Ou--0VWBoLD2beR2A
```

3.3 oauth2/token/{clientId}/{grantType}/{clientSecret}/{code} :

Une fois que le web service d'autorisation oauth2/authorize a retourné un token JWT signé avec le certificat communiqué entre TunTrust et l'AED en question pour assurer l'intégrité du contenu échangé, ce token doit être décodé et vérifié. Son identifiant unique « jti » est extrait par la suite pour servir en tant que paramètre « code » pour oauth2/token.

Ce web-service permet d'associer un jeton d'accès (sad) pour un utilisateur donné.

Le certificat avec lequel la signature du token jwt peut être vérifiée est le suivant :

```
-----BEGIN CERTIFICATE-----
MIIFSTCCAzGgAwIBAgIIW4u+9AWYVYYwDQYJKoZIhvcNAQELBQAwgYoxCzAJBgNV
BAYTAlROMS4wLAYDVQQKDCVOYXRpb25hbCBEaWdpdGFsIENlcnRpZmljYXRpb24g
QWdlbmN5MS4wLAYDVQQLDCVOYXRpb25hbCBEaWdpdGFsIENlcnRpZmljYXRpb24g
QWdlbmN5MRswGQYDVQQDDBJORENBIE1hbmFnZW1lbnQgQ0EwHhcNMTgxMDExMTMz
NDI0WhcNMjExMDEwMTMzNDI0WjCBjTELMAkGA1UEBhMCVE4xMjAwBgNVBAoMKU5h
dGlvbmFsIEFnZW5jeSBGb3IgRGlnaXRhbCBDZXJ0aWZpY2F0aW9uMTIwMAYDVQQL
DClOYXRpb25hbCBBZ2VuY3kgRm9yIERpZ2l0YWwgQ2VydGlmaWNhdGlvbjEWMBQG
A1UEAwwNYWRtaW4udHVuc2lnbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJgk2xvT1Zq0SqGLgJHdDJlNum/nJbTE1XRVrQa8LAd7kC3u8oDnAo5QRT+X
ZL4V1ohvGzcj5gYHe2JKlZofFr/UXqdeYfu5TlRn1SDTaiX1BUmVWtNBdWwkqJ5U
s4HVqIrxIEihAr6Ag5fQCVJ6uEvkey7a2pfTPPlbZ/dO96QTDGOCRH75SHKwxPgb
qPYIHcK2IaSudPJ5boAiVy+wZk4dTWnedF04P8HrRLtPqE6t0U/cPNsk6XvG1rhY
sfac5Nfh2+vUrXXvnzmIjq+11K27IlMj3e18HaZjHZrFJu0MyLZgZ9H58SYNRxtU
0gqea0UH2hIoYstatSwVdlFczVsCAwEAAaOBrTCBqjAdBgNVHQ4EFgQUrgxDTfpH
pe4MR6iKOiljfd2IhN8wDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBSZj4as3KW9
SuK2TQ6WHDOVyhv+zTARBgNVHSAECjAIMAYGBFUdIAAwDgYDVR0PAQH/BAQDAgWg
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAYBgNVHREEETAPgg1hZG1p
bi50dW5zaWduMA0GCSqGSIb3DQEBCwUAA4ICAQAtzhFGZLmP1lrXmC/cxhifBz4e
kmZfEK+Akl5pA60XSqjB4SnKlLrk7R/BMBc0iQPIJbSiR3BSLl8NmGwMe7PopdV3
VL5oUORgYU4m5P45jjjuecEJtl3A+W0v/tF9O/Nc1MICC08/AroenP9cxCyYRxsq
VfbPBjSrBG9v2wqDd2h0cZXF9P/BXL0ZDDdAgtuvvQOFVTwXCZHIvUCgqW85URlG
Zm8HVSQ3WCLH3+cBzGiPPdQOugp9fOQ3mkef0tCqTJefEXvdeua/1DOVFSnqNYQc
DggkHDyEH9X6cMPvRdiMKj1qs5Yv5AIp9djdKUNdpq1ik3SYKnKPHqu/JDBCf3sH
BOmrU4nItas2qTOUm+rMNbkb8Onim6wLVTnTE4Vzu6K/b0QI1nEsenHHPXCYFuz0
oemEKQ+242HwIxBu+guPpaTw60FW6qqE9oyBpTKp20/HAvVpSrKbdUdWOHvJCt2z
m7n+3nzNUI82YEGBK8VjFt9eomsHH6y0XGeFYx5JnOVaGXT38domAFYm2+Cvq43U
QcgJpUHt0m2fBA0IDYLBE38nyNaXP3s9rH5j8areaFdMrMB8Ytls9TaxRdbNBlZI
sazLa1H32wQAbmZU3mxY2pkkEVESIyx/TX/V79WZSpAiv1EDP1AGmo4D9ICreVen
U0tFLIWm4YnavH04TQ==
-----END CERTIFICATE-----
```

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/oauth2/token/{clientId}/{grantType}/{clientSecret}/{code}

Paramètre	Présence	Valeur	Description
grantType	OBLIGATOIRE (URL)	String	Ce paramètre prend la valeur de « authorization_code » , il est utilisé en cas d'autorisation par code.
Code	OBLIGATOIRE (URL)	string	Ce paramètre contient le code extrait du token d'autorisation (identifiant jti) retourné par le web-service **oauth2/authorize**. Il DOIT être lié à l'identifiant de l'AED et à l'URI de redirection.
clientSecret	OBLIGATOIRE (URL)	String	Code secret de l'AED attribué par Tuntrust.
clientId	OBLIGATOIRE (URL)	string	Ce paramètre correspond à l'identifiant de l'AED.
redirectUri	OBLIGATOIRE (BODY param)	string	Ce paramètre contient l'URI à laquelle est redirigé l'utilisateur après que le processus d'autorisation est finalisé. Il est utilisé pour valider qu'il correspond à la valeur d'origine précédemment transmise au serveur d'autorisation. Ceci NE DOIT être utilisé que si le paramètre redirectUri a été inclus dans la demande d'autorisation et leurs valeurs DOIVENT être identiques.

Output :

Paramètre	Présence	Valeur	Description
sad	OBLIGATOIRE	String	Ce paramètre contient un jeton d'accès de courte durée. Si scope= credential, le serveur d'autorisation renvoie un jeton de données d'activation de signature (**sad**) pour autoriser la demande de signature. Cette valeur DEVRAIT être utilisée comme valeur pour le paramètre **sad** lors de l'appel de la méthode **signatures/signHash**.
tokenType	OBLIGATOIRE	String	La valeur de ce paramètre est « **sad** ».
expiresIn	OPTIONAL	Number	Ce paramètre correspond à la durée de vie en secondes du jeton d'accès. La valeur par défaut est : 3600 sec.

Error Codes :

Error case	Status Code	Error	Error Description
Le paramètre "**grantType**" est vide	400 (bad Request)	invalid_request	Missing parameter **grantType**
Le paramètre " **grantType** " est invalide	400 (bad Request)	invalid_request	Invalid parameter **grantType**
Le paramètre "**code**" est vide	400 (bad Request)	invalid_request	Missing parameter **code**
Le paramètre "**code**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **code**
Le paramètre "**clientId**" est invalide	400 (bad Request)	invalid_request	Missing parameter **clientId**
Le paramètre " **clientId** " est invalide	400 (bad Request)	invalid_request	Invalid parameter **clientId**
Le paramètre "**clientSecret**" est vide	400 (bad Request)	invalid_request	Missing parameter **clientSecret**
Le paramètre "**clientSecret**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **clientSecret**
Le paramètre "**redirectUri**" est vide	400 (bad Request)	invalid_request	Missing parameter **redirectUri**
Le paramètre "**redirectUri**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **redirectUri**

Le paramètre "**redirectUri**" n'est pas associé au " clientId "	400 (bad Request)	invalid_request	RedirectUri not authorised for this AED.

Exemple de requête :

```
https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/oauth2/token/694b650c-eceb-4765-94f7-d170b4a9807a/authorization_code/123456789/decddc2d-0c1f-48f6-9fc0-3047f82c4c37
{
https://localhost:8443/pub/registration/token
}
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
    "sad": "1848ee79-d4aa-47d4-9ec9-5a943650dda8",
    "tokenType": "SAD",
    "expiresIn": 3600
}
```

3.4 signatures/signHash/{clientId}/{credentialId}/{sad}/{hashAlgo}/{ signAlgo}

Ce web service calcule la signature numérique à distance d'une ou plusieurs valeurs de hachage fournies en entrée. Cette méthode nécessite une autorisation d'identification sous la forme de données d'activation de signature (sad). L'application de signature doit d'abord passer à cette méthode le **sad** obtenu lors de l'appel des web services **oauth2/authorize** et **oauth2/token**.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/signatures/signHash/{clientId}/{credentialId}/{sad}/{hashAlgo}/{ signAlgo}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	string	Ce paramètre correspond à l'identifiant de l'AED.
credentialId	OBLIGATOIRE (URL)	string	Ce paramètre contient l'identifiant associé aux informations d'identification à autoriser (identifiant du porteur de certificat : email).
sad	OBLIGATOIRE (URL)	string	Ce paramètre contient le Signature Activation Data retourné par la fonction **oauth2/token**.
hash	OBLIGATOIRE (body param)	array of string	Ce paramètre contient une ou plusieurs valeurs d'empreintes (hash) à signer. Ce paramètre DOIT contenir le message brut encodé en Base64 digest (s).
hashAlgo	OBLIGATOIRE (URL)	string	Ce paramètre contient l'OID de l'algorithme de hachage utilisé lors du calcul de l'empreinte. Ce paramètre peut être ignoré si l'algorithme de hachage est spécifié dans le paramètre signAlgo. Seul les algorithmes de hashage > SHA256 peuvent être utilisés.
signAlgo	OBLIGATOIRE (URL)	string	Ce paramètre contient l'algorithme de signature à utiliser.

Output :

Paramètre	Présence	Valeur	Description
value	OBLIGATOIRE	Array of String	Un ou plusieurs hachage (s) signé (s) encodés en Base64. En cas de signatures multiples, les hachages signés DOIVENT être retournés dans le même ordre que les hachages correspondants fournis comme paramètre d'entrée.
algorithm	OBLIGATOIRE	string	Ce paramètre contient l'algorithme de signature utilisé lors de la signature du hash.

Error Codes :

Error case	Status Code	Error	Error Description
Le paramètre "**sad**" est vide	400 (bad Request)	invalid_request	Missing parameter **sad**
Le paramètre "**sad**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **sad**
Le paramètre "**credentialId**" est vide	400 (bad Request)	invalid_request	Missing parameter **credentialId**
Le paramètre "**credentialId**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **credentialId**
Le paramètre "**hash**" est invalide	400 (bad Request)	invalid_request	invalid type array parameter hash
Le paramètre "**hash**"est vide	400 (bad Request)	invalid_request	Empty hash array
Le paramètre "**hash**" est non autorisé	400 (bad Request)	invalid_request	Hash is not authorized by the SAD.
Le paramètre "**hashAlgo**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **hashAlgo**
La longueur du paramètre "**hash**" est invalide	400 (bad Request)	invalid_request	Invalid digest value length
Le paramètre "**sad**" est expiré	400 (bad Request)	invalid_request	SAD expired

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/signatures/signHash/694b650c-eceb-4765-94f7-d170b4a9807c/folen.benfoulen@certification.tn/b09bb8f0-828b-4328-ac0b-53865696acd3/SHA256/RSA
HTTP/1.1
Host: digigo.tuntrust.tn
Content-Type: application/json
Content-Type: text/plain
["LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ="]
```

Exemple de réponse :

```
HTTP/1.1 200 Found
 [
    {
      "algorithm": "RSA_SHA256",
      "value":
"bwu51FWVLDKHe0aAGDVoM2optPDc0/PomoLIAiHN01x0xCUMGR+NU9Qe5yQmRGO2VlQZb4SWCaCUmxKZvT3nEQ4TkxewHT31l+6//am2cUH2Ssfhy21Ped1jE7wmM3fRWqt3zCLCvYkGpdIWKkY7A…"
    }
]
```

3.5 credentials/extendTransaction/{clientId}/credentialId/{sad}

Ce web service permet de prolonger la validité d'une autorisation de transaction multi-signature en obtenant de nouvelles données d'activation de signature (**sad**). Cette méthode doit être utilisée en cas de transactions à signatures multiples lorsque la méthode **signatures/signHash** est invoquée plusieurs fois avec un seul **sad**.

Il peut également être utilisé pour renouveler un **sad**, avant son expiration, lorsque les opérations de signature prennent plus de temps que la valeur de **expiresIn** du **sad**. Un **sad** expiré ne peut pas être étendu.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/credentials/extendTransaction/{clientId}/credentialId/{sad}

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	string	Ce paramètre correspond à l'identifiant de l'AED.
credentialId	OBLIGATOIRE (URL)	string	email du signataire
hash	OBLIGATOIRE (body param)	array of string	Une ou plusieurs valeurs de hachage codées en Base64 à signer. Il permet au serveur de lier le nouveau **sad** à l'empreinte, empêchant ainsi l'utilisation d'une autorisation pour signer un contenu différent.
sad	OBLIGATOIRE (URL)	string	Ce paramètre contient le **sad** non expiré courant.

Output :

Paramètre	Présence	Valeur	Description
sad	OBLIGATOIRE	string	Ce paramètre contient le nouveau **sad**.
tokenType	OBLIGATOIRE	String « SAD »	La valeur de ce paramètre est SAD.
expiresIn	OPTIONAL	Number	Ce paramètre correspond à la durée de vie en secondes du nouveau jeton d'accès « **sad** ». La valeur par défaut est : 3600 sec.

Error Codes :

Error case	Status Code	Error	Error Description
Le paramètre "**credentialId**" est vide	400 (bad Request)	invalid_request	Missing string parameter **credentialId**
Le paramètre "**credentialId**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **credentialId**
Le paramètre "**hash**" est vide	400 (bad Request)	invalid_request	Missing string parameter **hash**
Le paramètre "**hash**" est invalide	400 (bad Request)	invalid_request	Invalid parameter **hash**
La longueur du paramètre "**hash**" est invalide	400 (bad Request)	invalid_request	Invalid digest value length
Le paramètre "**hash**" est non autorisé	400 (bad Request)	invalid_request	**Hash** is not authorized by the sad.
Le paramètre "**sad**" est vide	400 (bad Request) (bad request)	invalid_request	Missing string parameter **sad**
Le paramètre "sad" est invalide	400 (bad Request) (bad request)	invalid_request	Invalid parameter **sad**

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-
webapp/services/v1/credentials/extendTransaction/694b650c-eceb-4765-94f7-
d170b4a1247c/foolen.benfoulen@certification.tn/1848ee79-d4aa-47d4-9ec9-5a943650dda8
 HTTP/1.1
Host: digigo.tuntrust.tn
Content-Type: application/json

["iC4bF97Gg8H0pKNGL/6OypKfECVAt+a9GL7lLyPTjYE=","n4bQgYhMfWWaL+qgxVrQFaO/TxsrC4Is0V1sFbDwCgg="]
```

Exemple de réponse :

```
HTTP/1.1 200 Found
{
    "sad": "4190f677-5ac7-4a23-bf6c-c0a234c81dea",
    "tokenType": "SAD",
    "expiresIn": 3600
}
```

3.6 Timestamp/{clientId}/{hashAlgo}

Ce web service permet de générer un jeton d'horodatage pour la valeur de hachage donnée en entrée.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/v1/signatures/timestamp/694b650c-eceb-4765-94f7-d170b4a1247c/SHA256

Paramètre	Présence	Valeur	Description
clientId	OBLIGATOIRE (URL)	string	Ce paramètre correspond à l'identifiant de l'AED.
hash	OBLIGATOIRE (BodyParam)	String	Ce paramètre contient la valeur de l'empreinte encodée en Base64 à horodater. L'AED doit utiliser cette valeur pour coder la valeur de MessageImprint.hashedMessage comme défini dans la RFC 3161.
hashAlgo	OBLIGATOIRE (URL)	String	Ce paramètre contient l'OID de l'algorithme de hachage utilisé lors du calcul de l'empreinte. Ce paramètre peut être ignoré si l'algorithme de hachage est spécifié dans le paramètre signAlgo. Seuls les algorithmes de hashage > SHA256 peuvent être utilisés.
nonce	OPTIONEL	String	Ce paramètre contient un grand nombre aléatoire avec une forte probabilité qu'il ne soit généré qu'une seule fois par l'application de signature. La valeur DOIT être représentée sous la forme d'une chaîne codée hexadécimale.

Output :

Paramètre	Présence	Valeur	Description
timestamp	OBLIGATOIRE	string	Le jeton d'horodatage codé en Base64 tel que défini dans la RFC 3161 mise à jour par la RFC 5816. Si le paramètre nonce est inclus dans la demande, il DOIT également être inclus dans le jeton d'horodatage, sinon la réponse DEVRA être rejetée.

Error Codes :

Error case	Status Code	Error	Error Description
Le paramètre "**hash**" est invalide	400 (bad Request)	invalid_request	Invalid type parameter **hash**
Le paramètre "**hash**" est vide	400 (bad Request)	invalid_request	Empty **hash** array
Le paramètre "**hash**" est non autorisé	400 (bad Request)	invalid_request	**Hash** is not authorized by the SAD.
Invalid "**hashAlgo**" parameter	400 (bad Request)	invalid_request	Invalid parameter **hashAlgo**

La longueur du **hash** est invalide	400 (bad Request)	invalid_request	Invalid digest value length

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-
webapp/services/v1/signatures/timestamp/694b650c-eceb-4765-94f7-d170b4a1247c/SHA256
HTTP/1.1
Host: digigo.tuntrust.tn
Content-Type: application/json

01ICvILo/Wx+BqB5YT2AM433m/WnnwRsTNVBKZ0uHic=
```

Exemple de réponse :

```
MIAGCSqGSIb3DQEHAqCAMIIibQIBAzEPMA0GCWCGSAFlAwQCAQUAMIH4BgsqhkiG9w0BCRABBKCB6ASB5TCB4gIBAQYGBAC
PZwEBMDEwDQYJYIZIAWUDBAIBBQAEINNSAryC6P1sfgageWE9gDON95v1p58EbEzVQSmdLh4nAghgCNrhENC8uBgPMjAyMD
AzMDIxNDE1NThaMAMCAQGgZaRjMGExCzAJBgNVBAYTAlROMTcwNQYDVQQKDC5BR0VOQ0UgTkFUSU9OQUxFIERFIENFUlRJR
klDQVRJT04gRUxFQ1RST05JUVVFMRkwFwYDVQQDDBBYXRpb24gQWdlbmN5MRcwFQYDVQQDDA5UblRydXN0IEdvdiBDQTAeF
w0xOTEyMDYwODAyNDBaFw0yMjEyMDUwODAyNDBaMGExCzAJBgNVBAYTAlROMTcwNQYDVQQK…
```

4 Valider la signature d'un document

Ce web service permet de valider la signature d'un document.

Input :

https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy/validate-signature

Paramètre	Sous paramètre	Présence	Valeur	Description
signedDocument				
	bytes	OBLIGATOIRE	String	Ce paramètre contient le document signé en base64 à valider.
	Name	OPTIONEL	String	Ce paramètre contient le nom du document signé.
	mimeTypeString	OBLIGATOIRE	mimeTypeString	Ce paramètre correspond au type du document à valider : • text/pdf • text/xml
		originalDocuments		
	bytes	CONDITIONNEL	String	Ce paramètre contient le document original en base64 dans le cas d'une signature détachée.
	Name	OPTIONEL	String	Ce paramètre contient le nom du document original dans le cas d'une signature détachée.
	mimeTypeString	CONDITIONNEL	mimeTypeString	Ce paramètre correspond au type du document original dans le cas d'une signature détachée: • text/pdf • text/xml • …
policy		OPTIONEL	String	Ce paramètre contient la politique de validation.
signatureId		OPTIONEL	String	Ce paramètre contient l'identifiant de la signature à valider.

Output :

Paramètre	Présence	Valeur	Description
validationReport	OBLIGATOIRE	string	Le rapport de validation de signature sous format Json. Ce rapport se compose de trois parties : • diagnosticData • simpleReport • detailedReport Si la signature est valide et le certificat du signataire est valide, l'état de validation de signature est affiché dans le paramètre « indication » : • TOTAL_PASSED • TOTAL_FAILED • INDETERMINATE Dans le cas de TOTAL_FAILED et INDETERMINATE, une sous indication représentant la raison pour laquelle la validation a eu le résultat en question.

Exemple de requête :

```
POST https://digigo.tuntrust.tn/tunsign-proxy-webapp/services/rest/tunsign-proxy/validate-signature
HTTP/1.1
Host: digigo.tuntrust.tn
Content-Type: application/json
{
            "signedDocument":
            {
                  "bytes":"JVBERi0xLjMKMyAwIG9iago8PC9UeXBlIC9QYWdlCi9QYXJlbnQgMSAwI…",
                  "name":"signed.pdf",
                  "mimeType": {
                        "mimeTypeString":"text/pdf"
                  }
            },
            "originalDocuments" : [],
            "policy" : null,
            "signatureId" : null
}
```

Exemple de réponse :

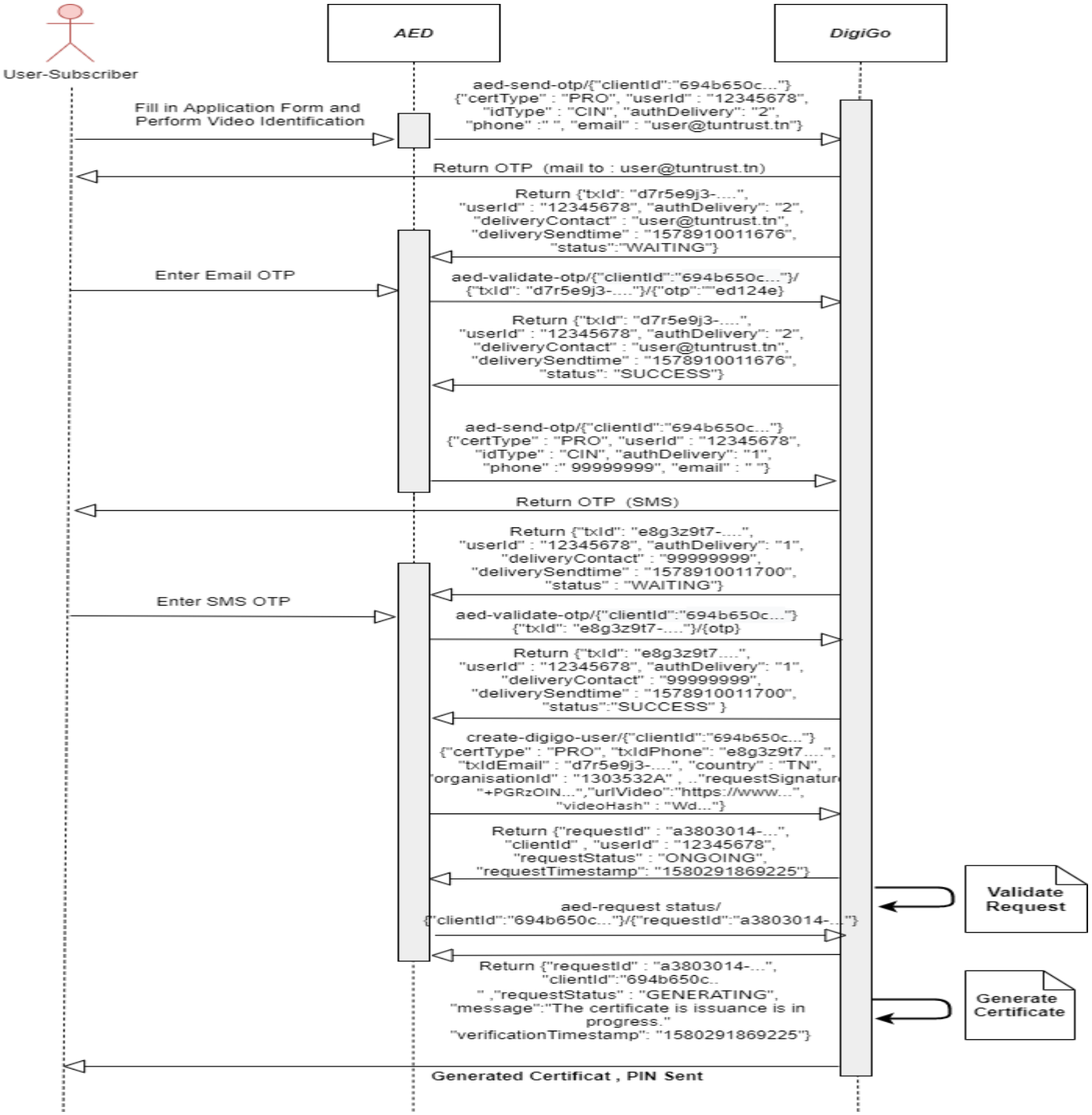
```
{
    "diagnosticData": {
    …
    },
    "simpleReport": {
        "policy": {
            "policyName": "QES AdESQC TL based",
            "policyDescription": "Validate electronic signatures ..."
        },
        "validationTime": 1591776481961,
        "documentName": "signed.pdf",
        "validSignaturesCount": 0,
        "signaturesCount": 1,
        "containerType": null,
        "signature": [
            {
                "filename": null,
                "signingTime": 1574198296000,
                "bestSignatureTime": 1591776481961,
                "signedBy": "Foulen ben foulen",
                "certificateChain": {
                    "certificate": [
                        {
                            "id":
"297E3711615CAE98D45462A4B47E42B73F70A26DE57DE7699EDF714710B3468D",
                            "qualifiedName": "Foulen ben foulen "
                        },
                        {
                            "id":
"05E91E22D19D5097EC9346E7CA4E17E96EAD4CCB1C2861045485FC4A711D5F2B",
                            "qualifiedName": "NDCA Management CA"
                        }
                    ]
                },
                "signatureLevel": {
                    "value": "NA",
                    "description": "Not applicable"
                },
                "indication": "INDETERMINATE",
                "subIndication": "NO_CERTIFICATE_CHAIN_FOUND",
                "errors": [
                    "The certificate path is not trusted!",
                    "The result of the LTV validation process is not acceptable to continue
the process!"
```

```
                ],
                "warnings": [
                    "The signature/seal is an INDETERMINATE AdES!"
                ],
                "infos": [],
                "signatureScope": [
                    {
                        "value": "Full document",
                        "name": "Full PDF",
                        "scope": "FULL"
                    }
                ],
                "id": "id-97267f3f661527f1e0d9862fafc0b064e40a1754bad3bc8e4233e4747fd38164",
                "counterSignature": null,
                "parentId": null,
                "signatureFormat": "PAdES-BASELINE-B"
            }
        ]
    },
    "detailedReport": {
    …
    }
}
```

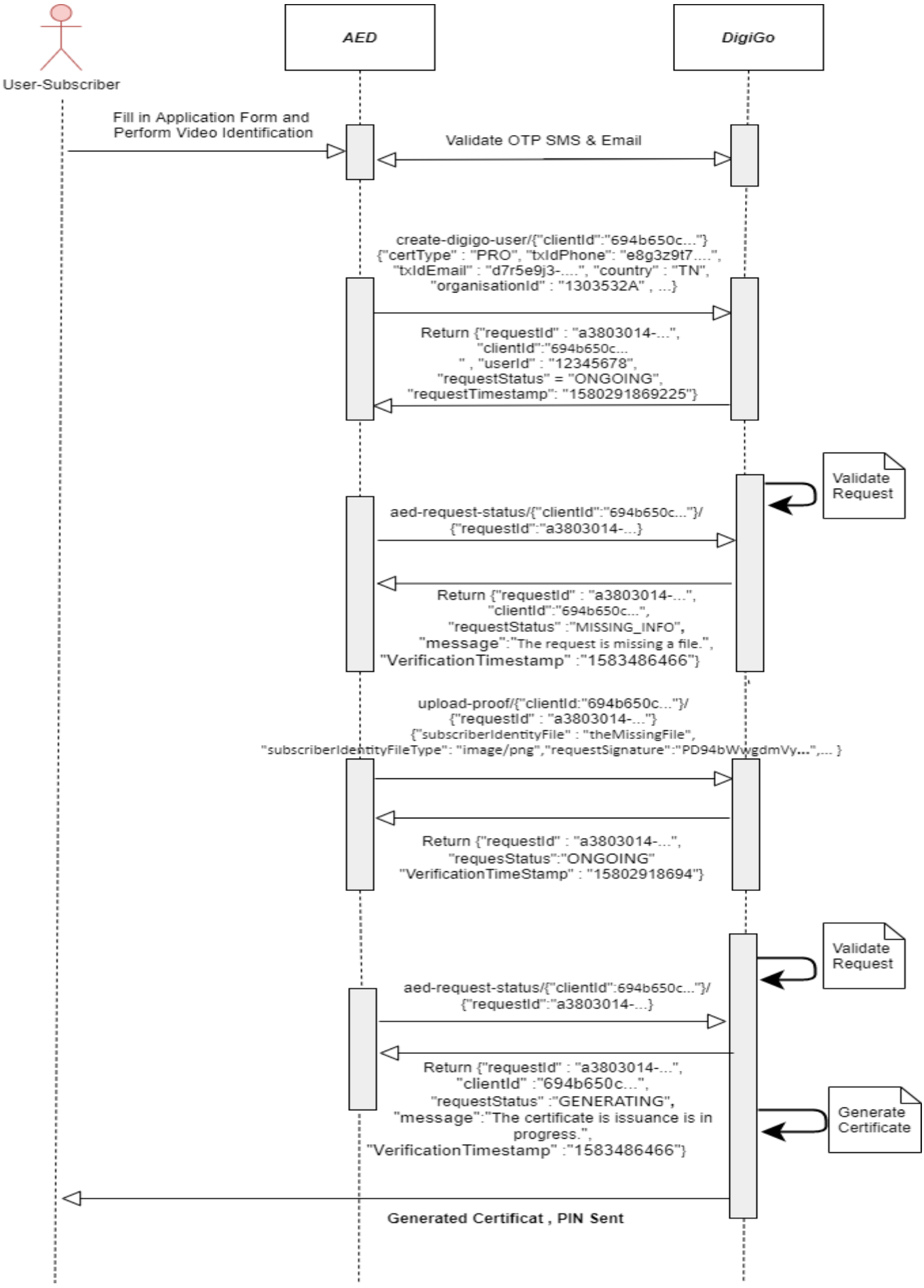
5 Diagrammes de Séquences

Cette section permet de représenter les interactions avec et au sein de l'API Digigo :

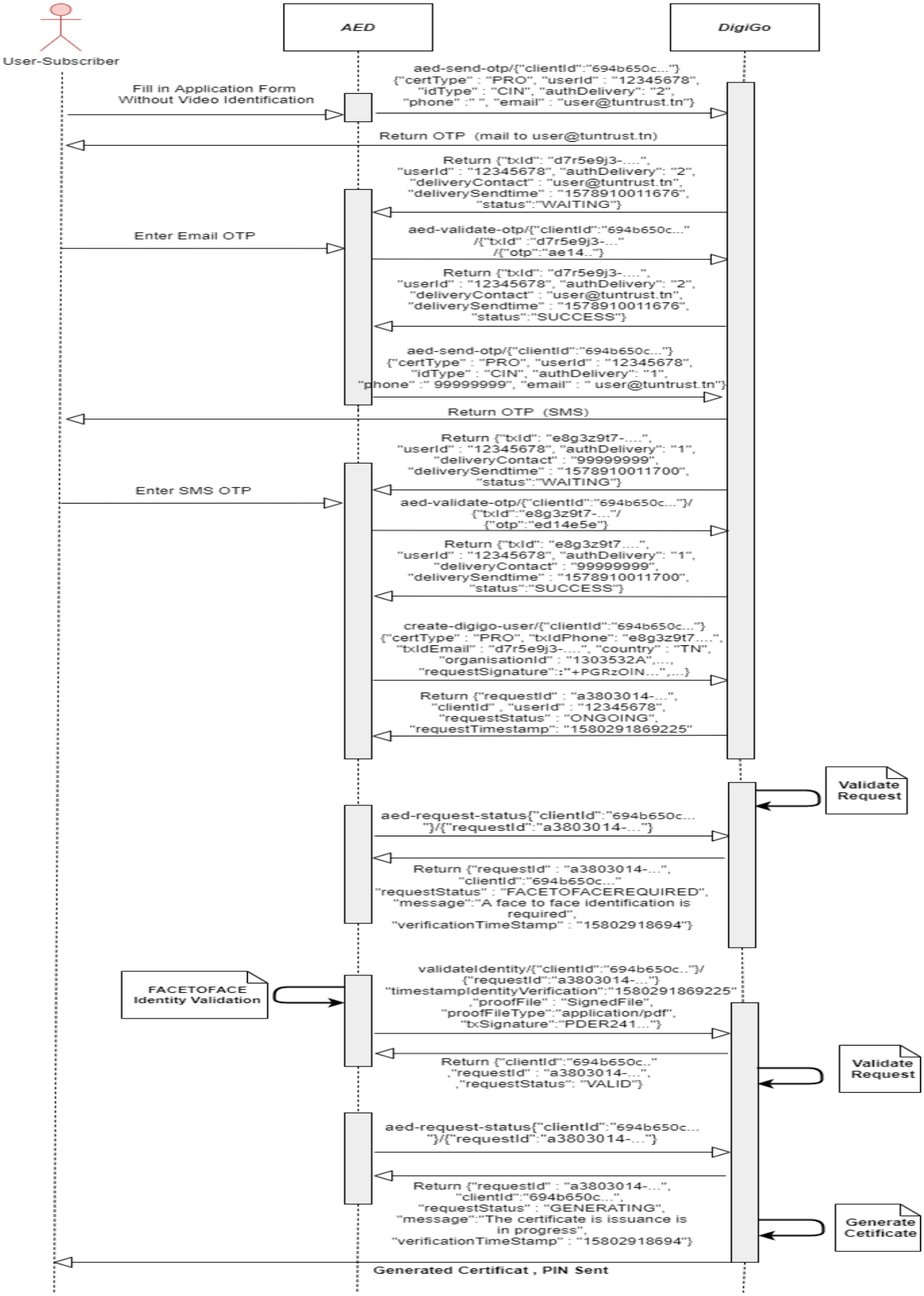
5.1 Diagramme AED-Inscription



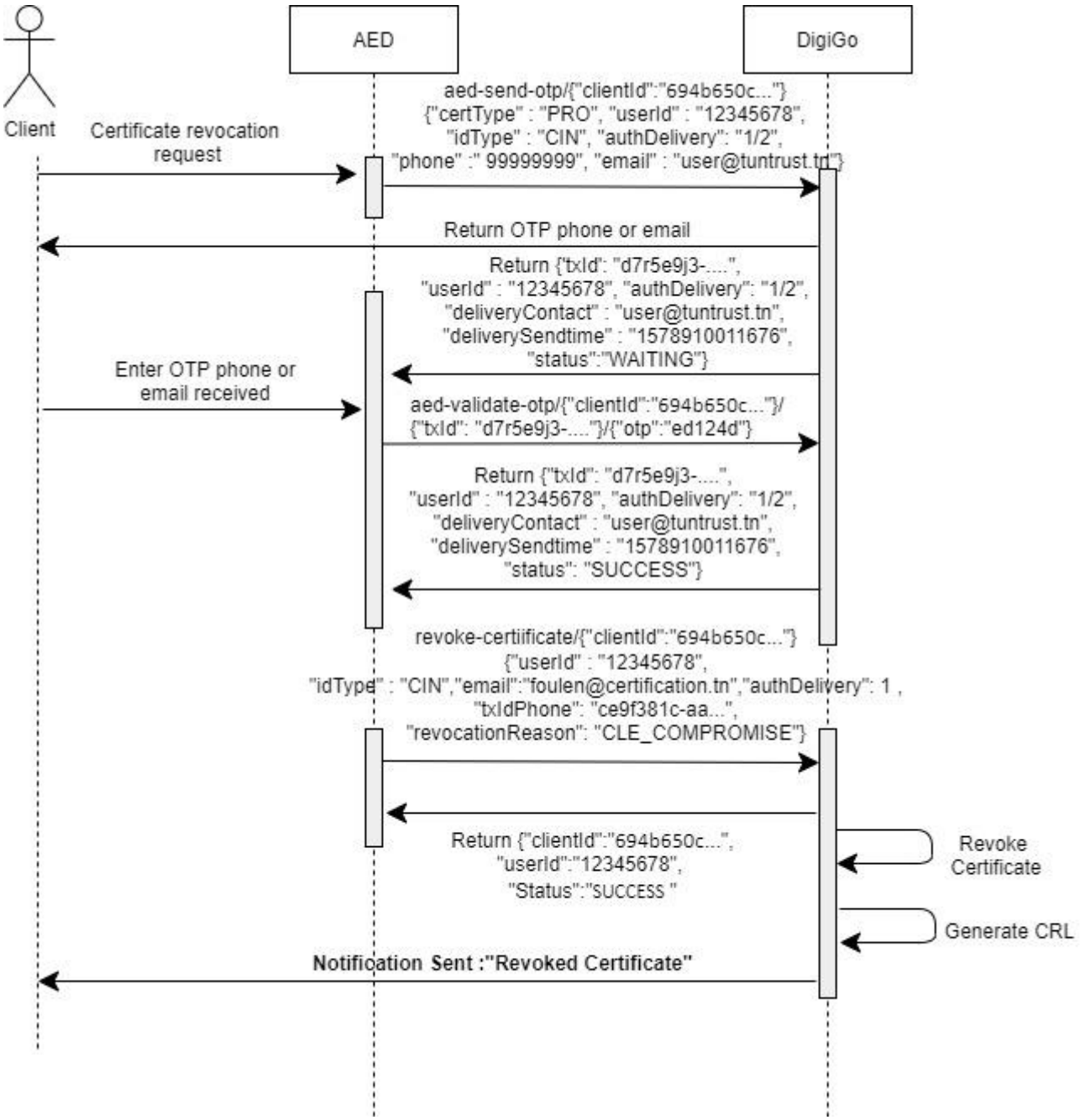
5.2 Diagrammes Aed-Inscription With Missing File



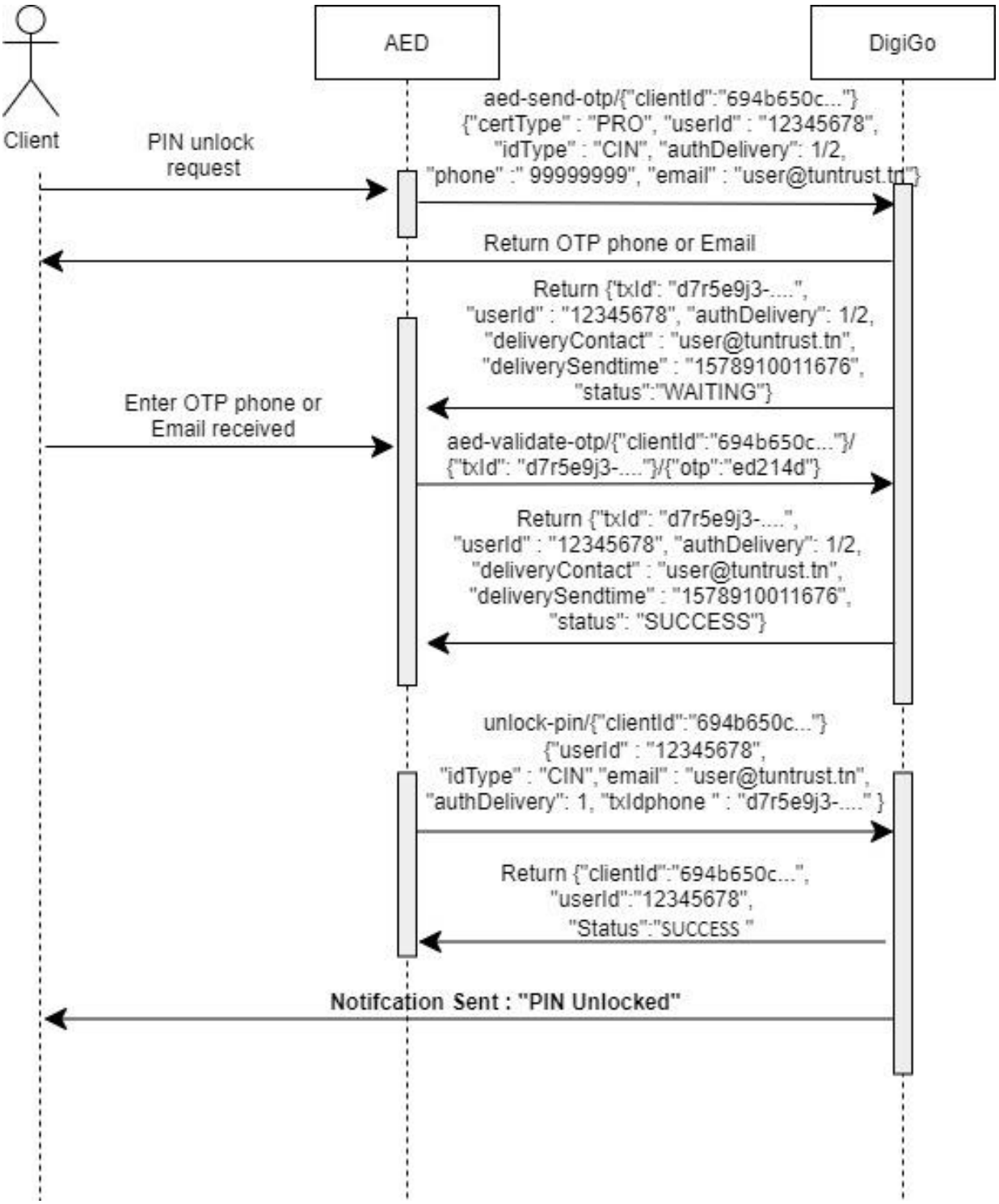
5.3 Diagrammes Aed-Inscription-FaceToFace Required



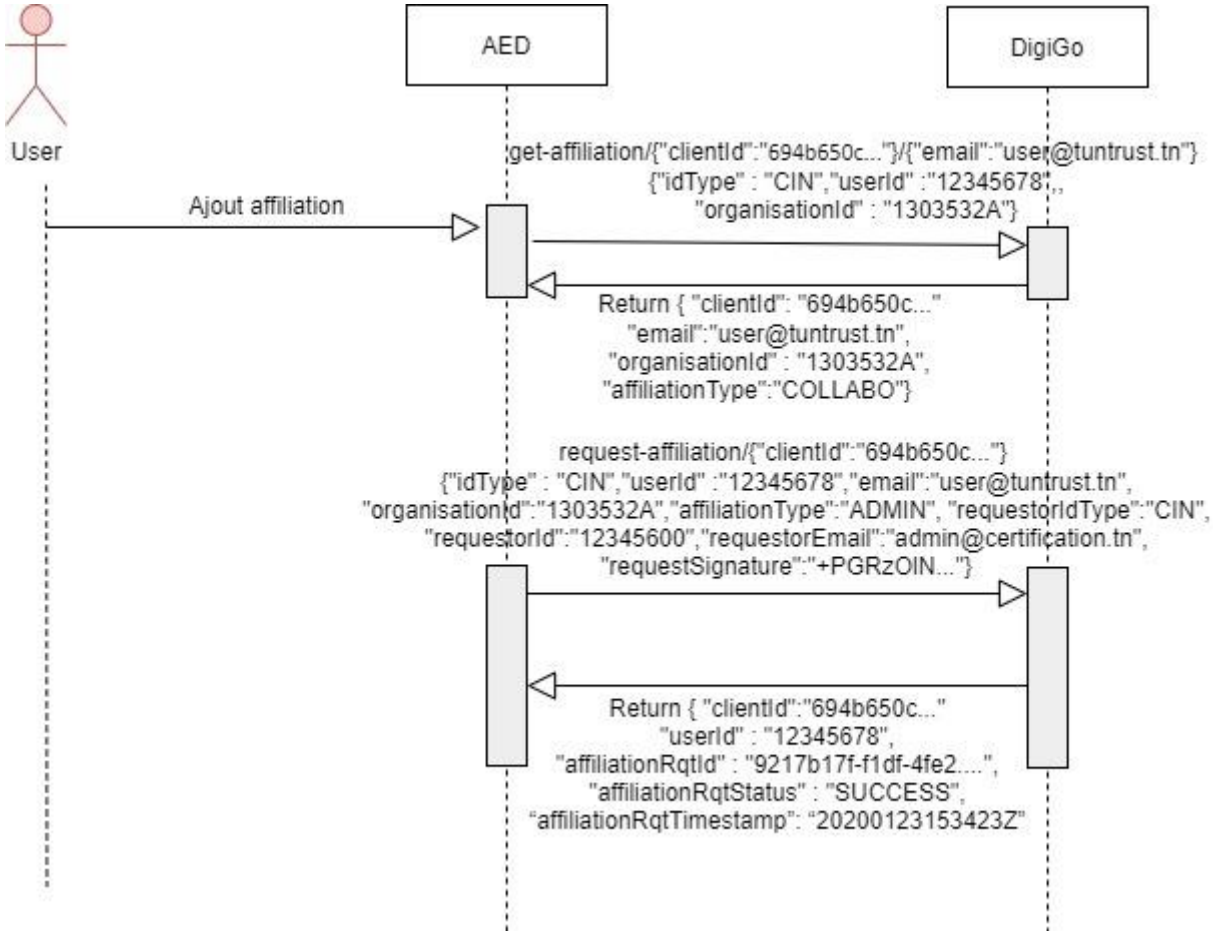
5.4 Diagramme Revoke certificate



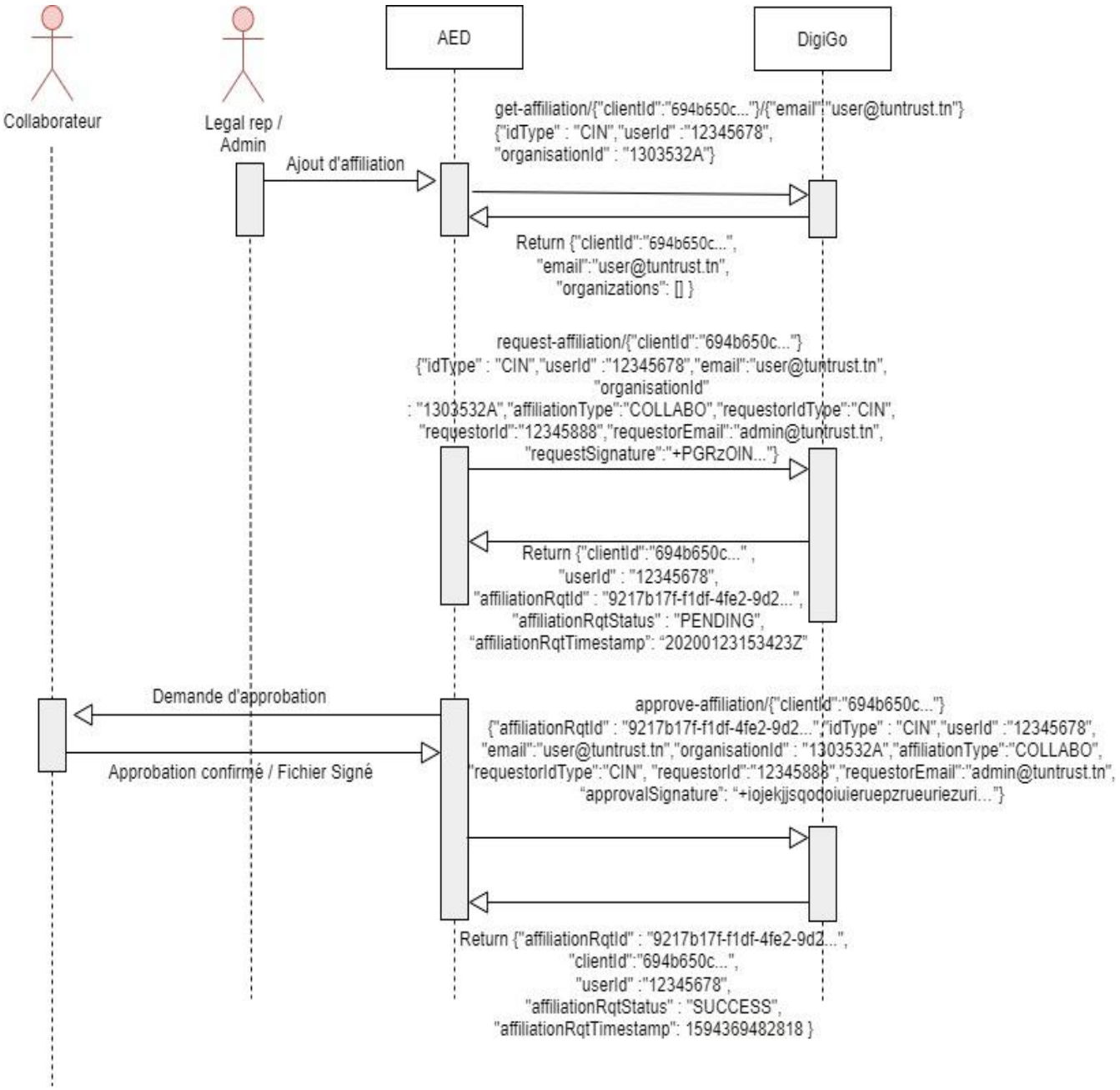
5.5 Diagramme unlock PIN



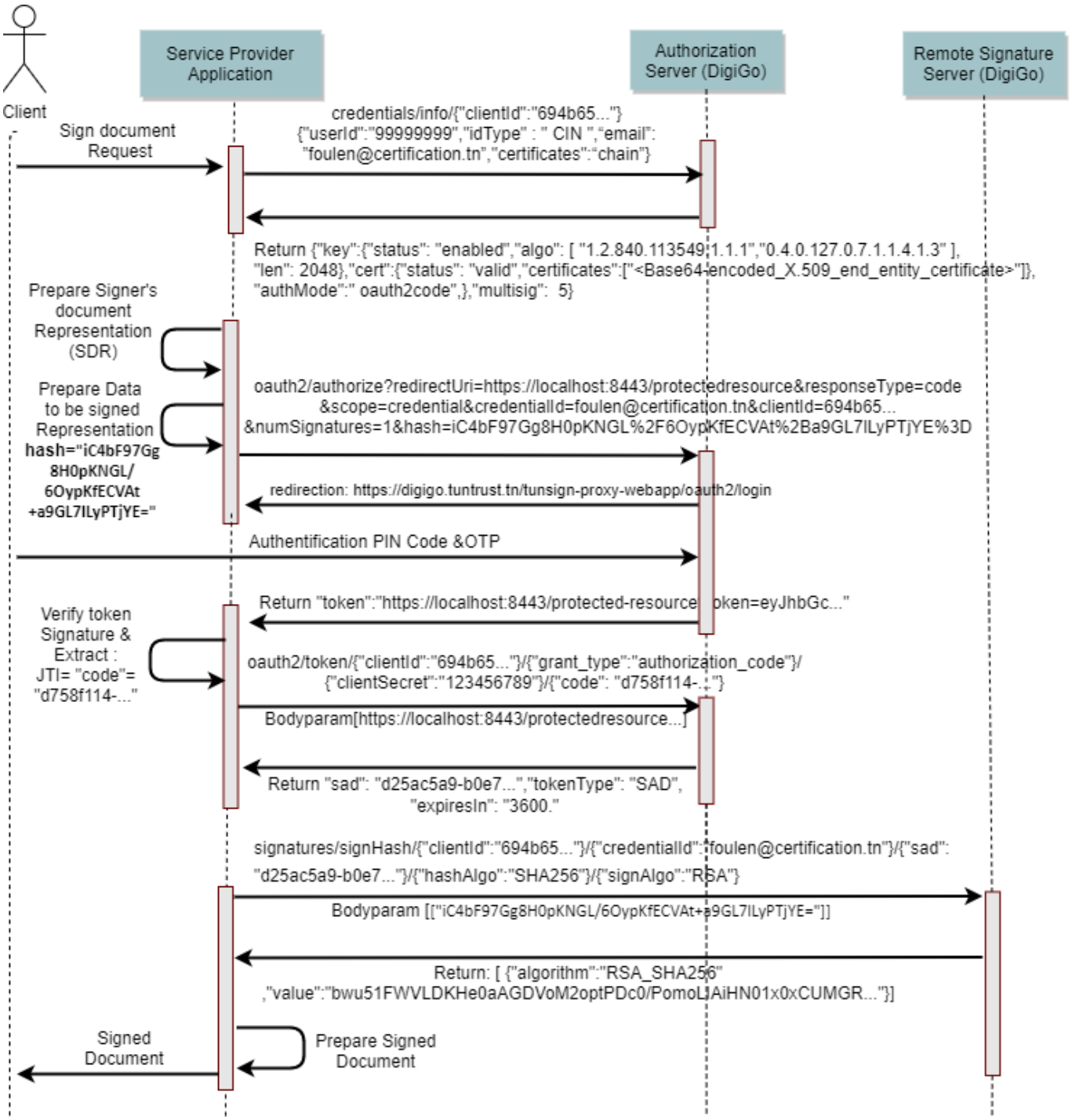
5.6 Diagramme ajout affiliation cas d'un représentant légal ou administrateur



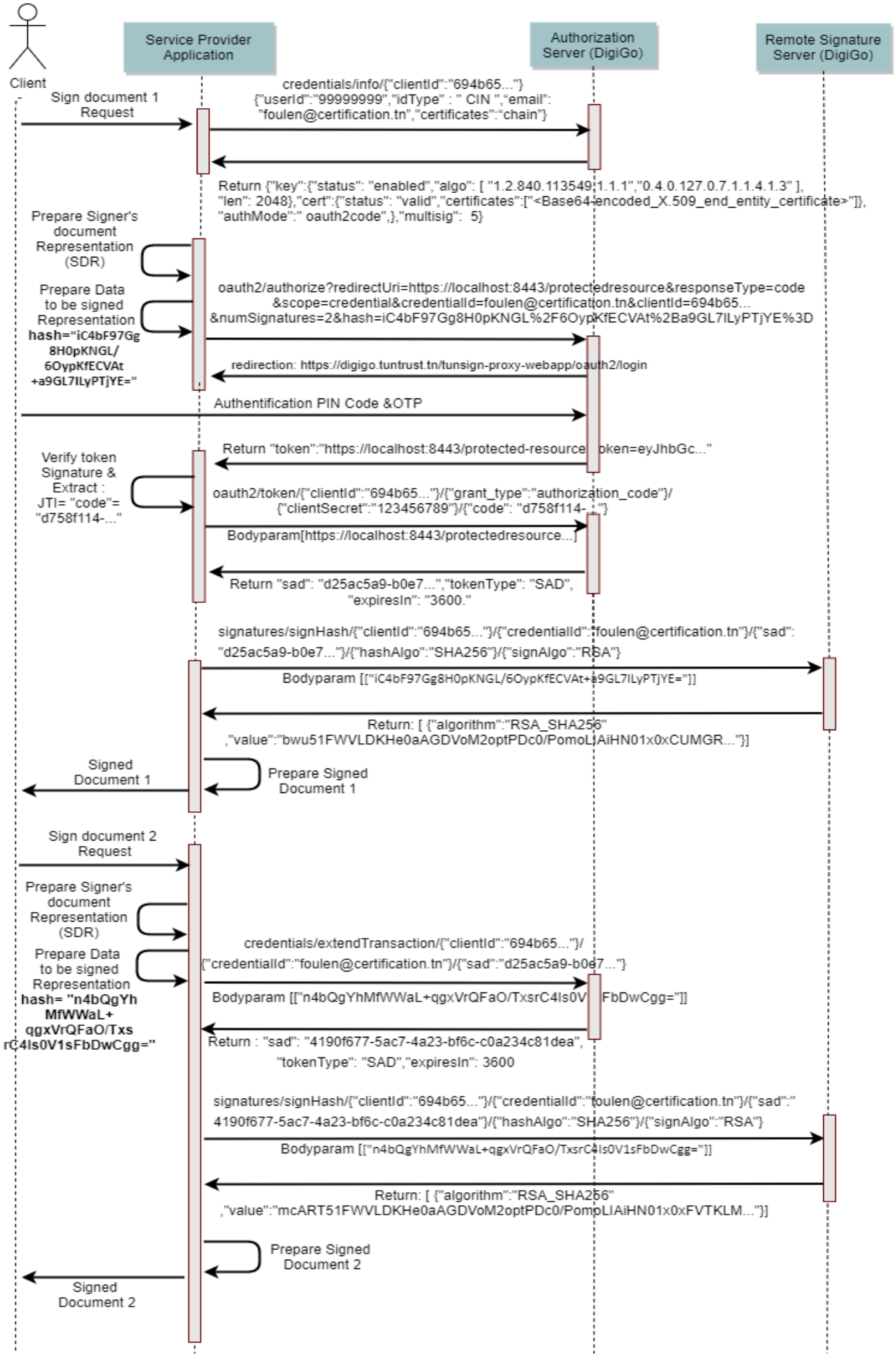
5.7 Diagramme ajout affiliation cas d'un collaborateur



5.8 Diagramme de signature d'un Hash



5.9 Diagrammes de signature de plusieurs Hashs



Annexe 1 : Formulaire de demande

Information sur l' entité			
Identifiant Unique			
Raison Sociale			
Adresse de l'entité			
N°, Rue, App			
Code postal		**Ville**	
Gouvernorat		**Pays**	
Information sur le représentant légal			
Nom et Prénom			
N°Pièce d'identité		☐ CIN ☐ Passeport ☐ Permis de séjour	
Tél. professionnel			
Email professionnel			
Information sur le demandeur			
Nom et Prénom			
N°Pièce d'identité		☐ CIN ☐ Passeport ☐ Permis de séjour	
Fonction			
Tél. professionnel		**Mobile**	
Email professionnel			
Domaine d'utilisation	**☐ CNSS ☐ E-JEBAYA ☐ CCPNET ☐ TTN ☐ Autres:**		
	Tuneps : ☐ Fournisseur ☐ Gestionnaire ☐ Acheteur Public(*)		