Guide d'Intégration de la signature électronique Universign

VERSION : 1.5	DIFFUSION : *PUBLIQUE*	17/06/2021

Table des Matières

1 Introduction

Ce « Guide d'Intégration de la Signature Electronique Universign » a pour objectif de présenter des exemples d'intégration de la solution de signature Universign. Il est destiné à nos clients dans le cadre d'une mise en place de la signature électronique de niveau simple (1) ou certifié (2). Plusieurs cas d'usage sont traités d'un point de vue fonctionnel et technique.

Les exemples d'intégration traités sont les suivants :

- Un document à signer de **niveau simple** par un signataire
- Un document à signer de niveau simple par un signataire avec l'utilisation d'un **cachet serveur**
- Un document à signer de **niveau certifié** par un signataire
- La **pré-validation** en vue de l'émission d'un certificat de personne physique.
- L'émission d'un certificat de personne physique en **Standalone**

Pour les cas utilisant de mise en place d'autres niveaux de signature, nous vous invitons à contacter votre contact commercial afin de définir le mode d'accompagnement le plus adapté à vos besoins.

2 Principes de la signature électronique Universign

La signature électronique Universign consiste à faire signer un ou plusieurs documents au format PDF à une ou plusieurs personnes physiques ou morales de manière dématérialisée. Le processus de signature électronique utilisé garantit l'intégrité du document et permet d'identifier les signataires ayant signé les documents, comme pour une signature de documents au format papier.

Une définition complète est disponible sur notre page dédiée au Support :

https://help.universign.com/hc/fr/articles/200256402-Qu-est-ce-qu-une-signature-%C3%A9lectronique-

Universign propose plusieurs niveaux de signature qui sont liés au niveau d'identification des signataires :

- Signature simple (niveau 1)
- Signature certifiée (niveau 2)
- Signature avancée avec certificat qualifié (niveau 3)
- Signature avec certificat de personne morale (cachet serveur)

	Signature niveau 1	Signature niveau 2	Signature niveau 3
eIDAS	Signature simple*	Signature avancée	Signature avancée avec certificat qualifié
Normes européennes	TS : EN 319 421 EC : EN 319 411-1 *TS : Horodatage* *EC : Emission de Certificat*	TS : EN 319 421 EC : EN 319 411-1 LCP ***Attention :*** *les normes EN 319 411/421 remplacent les standard TS 102 023/042 et EN 101 456*	TS : EN 319 421 EC : EN 319 411-2 QCP-n
Intégrité	Horodatage qualifié	Horodatage qualifié	Horodatage qualifié
Identité	Authentification simple ou délégué Fichier de preuve	Authentification double facteur Fichier de preuve Vérification de la pièce d'identité	Authentification double facteur Fichier de preuve Vérification de la pièce d'identité + Face à face
Certificat	Pas de certificat nominatif	Certificat nominatif	Certificat nominatif qualifié
Valeur juridique			

** peut-être une signature avancée sous réserve des procédés d'identification mis en œuvre par le client*

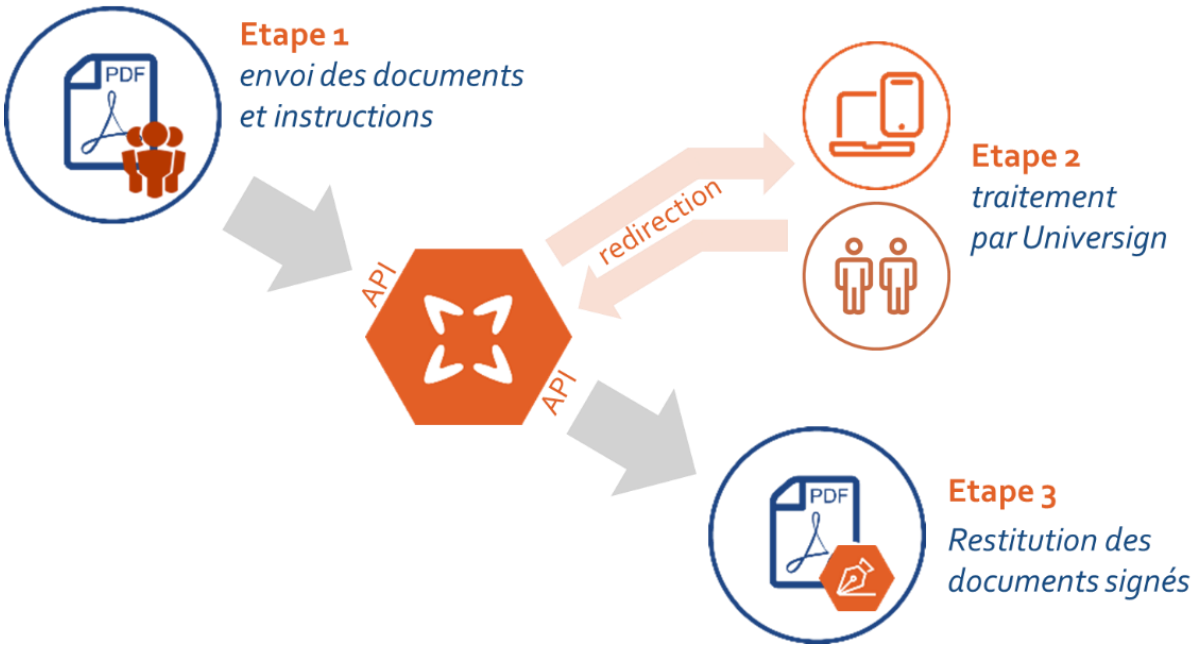
Chaque cycle de signature est appelé **collecte** ou **transaction**.

Les termes utilisés sont définis dans la page dédiée au Support : https://help.universign.com/hc/fr

3 Intégration fonctionnelle de la signature électronique

La mise en place de la signature électronique intervient en général dans le cadre de la digitalisation des processus de contractualisation ou de validation de documents. Il est important de définir à quels moments du processus la signature électronique intervient.

Le processus de la signature électronique peut être décrit selon 3 étapes :



4 Intégration API

4.1 Protocole utilisé

Le protocole XML-RPC est utilisé pour appeler nos API Universign.

L'url de connexion sur la plateforme de recette est : https://sign.test.cryptolog.com/sign/rpc/

L'url de connexion sur la plateforme de production est : https://ws.universign.eu/sign/rpc/

L'ensemble des méthodes utilisées décrit dans le guide Universign mis à jour régulièrement.

4.2 Compte Universign

Pour utiliser l'API Universign, vous devez ouvrir un compte. Durant ce processus d'ouverture de compte, un compte administrateur (email + mot de passe) vous permettant d'appeler les API Universign, vous sera communiqué.

Les Url permettant de créer un compte sur nos plateformes sont :

- Recette : https://sign.test.universign.eu/fr/signup/
- Production : https://app.universign.com/fr/signup/

Les Url permettant d'accéder à votre compte sur nos plateformes sont :

- Recette : https://sign.test.universign.eu/fr/signin/
- Production : https://app.universign.com/fr/signin/

L'appel sur la plateforme de recette se fait de la façon suivante :

https://[LOGIN]:[PASSWORD]@sign.test.cryptolog.com/sign/rpc/

Sur la plateforme de production l'appel est :

https://[LOGIN]:[PASSWORD]@ws.universign.eu/sign/rpc/

Ce compte administrateur est rattaché à une organisation dont le libellé correspond en général au nom de votre société. Ce compte vous permet d'accéder à l'interface Web afin de gérer de manière fonctionnelle l'état d'avancement d'une collecte depuis la création jusqu'à la réception des documents signés.

A la création de votre compte, un profil de signature par défaut appelé « default » est associé.

4.3 Navigateurs WEB non supportés

Le tableau ci-dessous liste les versions de navigateur non supportées par Universign.

Navigateur	Version de navigateur
Internet Explorer	< 11
Chrome	< 29
Firefox	< 29
Safari	< 9
Samsung Internet for Android	< 5
Opera	< 16

5 Création d'une collecte de signature

5.1 La structure d'une collecte

La création d'une collecte consiste en la création et l'envoi d'une requête en XML-RPC vers les serveurs Universign.

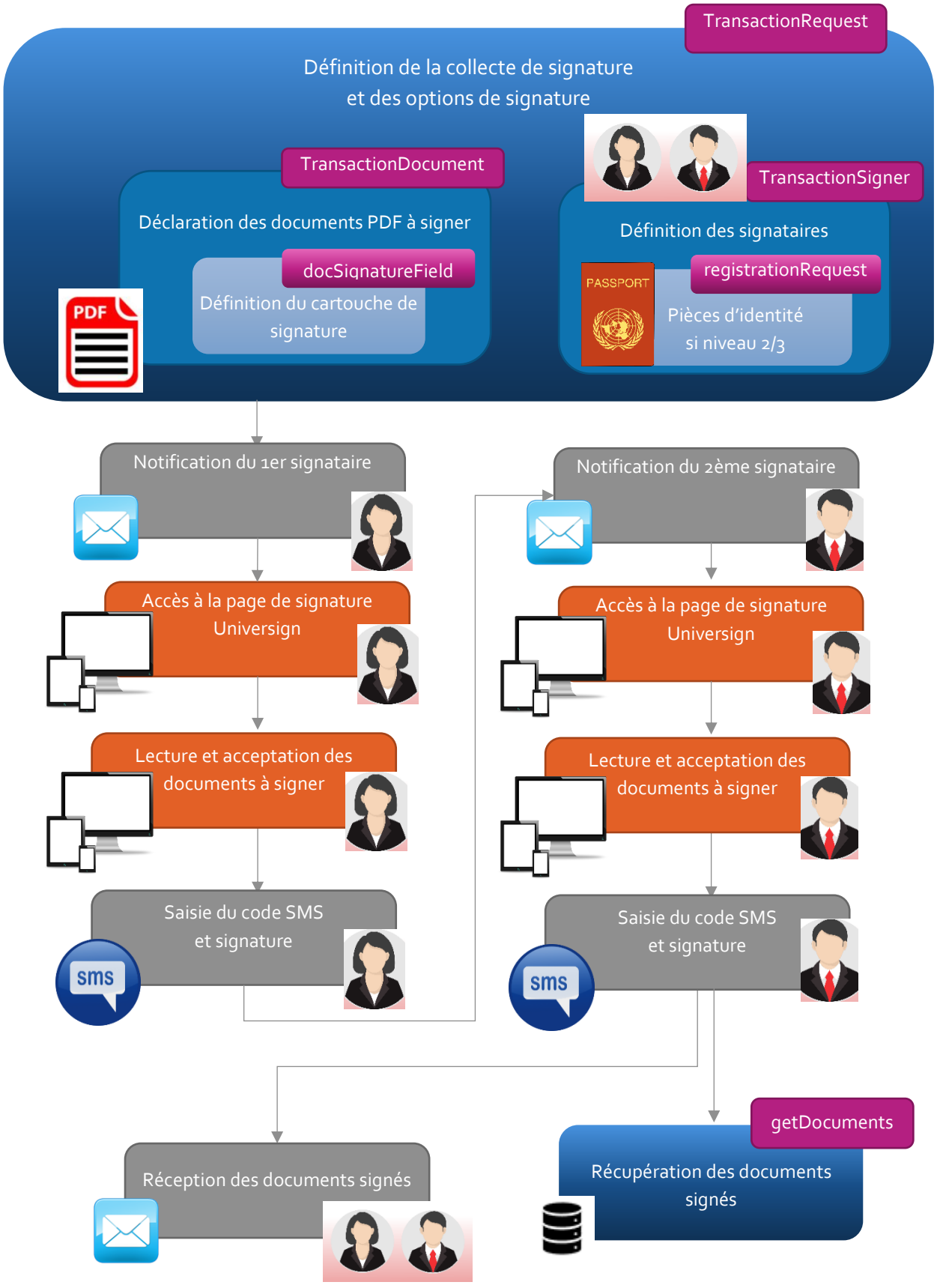
Une collecte se compose des éléments suivants :

- Un ou plusieurs **signataires**.
- Un ou plusieurs **documents** et leurs cachets de signatures.
- Des **options** portant sur :
    - La cinématique de signature,
    - Les URLs de redirection,
    - Le niveau de signature,
    - La langue utilisée,
    - ...

Il n'est pas possible de modifier, d'ajouter ou supprimer des signataires ou des documents, ni même les options de signataire une fois la requête envoyée au serveur.

Le parcours fonctionnel de signature pour 2 signataires peut être représenté de la façon suivante : code couleur :

Appels API Universign
Méthodes et structures utilisées
Notifications
Page de signature Universign


TransactionRequest
Définition de la collecte de signature
et des options de signature
TransactionDocument
Déclaration des documents PDF à signer
docSignatureField
Définition du cartouche de signature
PDF
TransactionSigner
Définition des signataires
registrationRequest
PASSPORT
Pièces d'identité si niveau 2/3
Notification du 1er signataire
Accès à la page de signature Universign
Lecture et acceptation des documents à signer
Saisie du code SMS et signature
sms
Notification du 2ème signataire
Accès à la page de signature Universign
Lecture et acceptation des documents à signer
Saisie du code SMS et signature
sms
Réception des documents signés
getDocuments
Récupération des documents signés

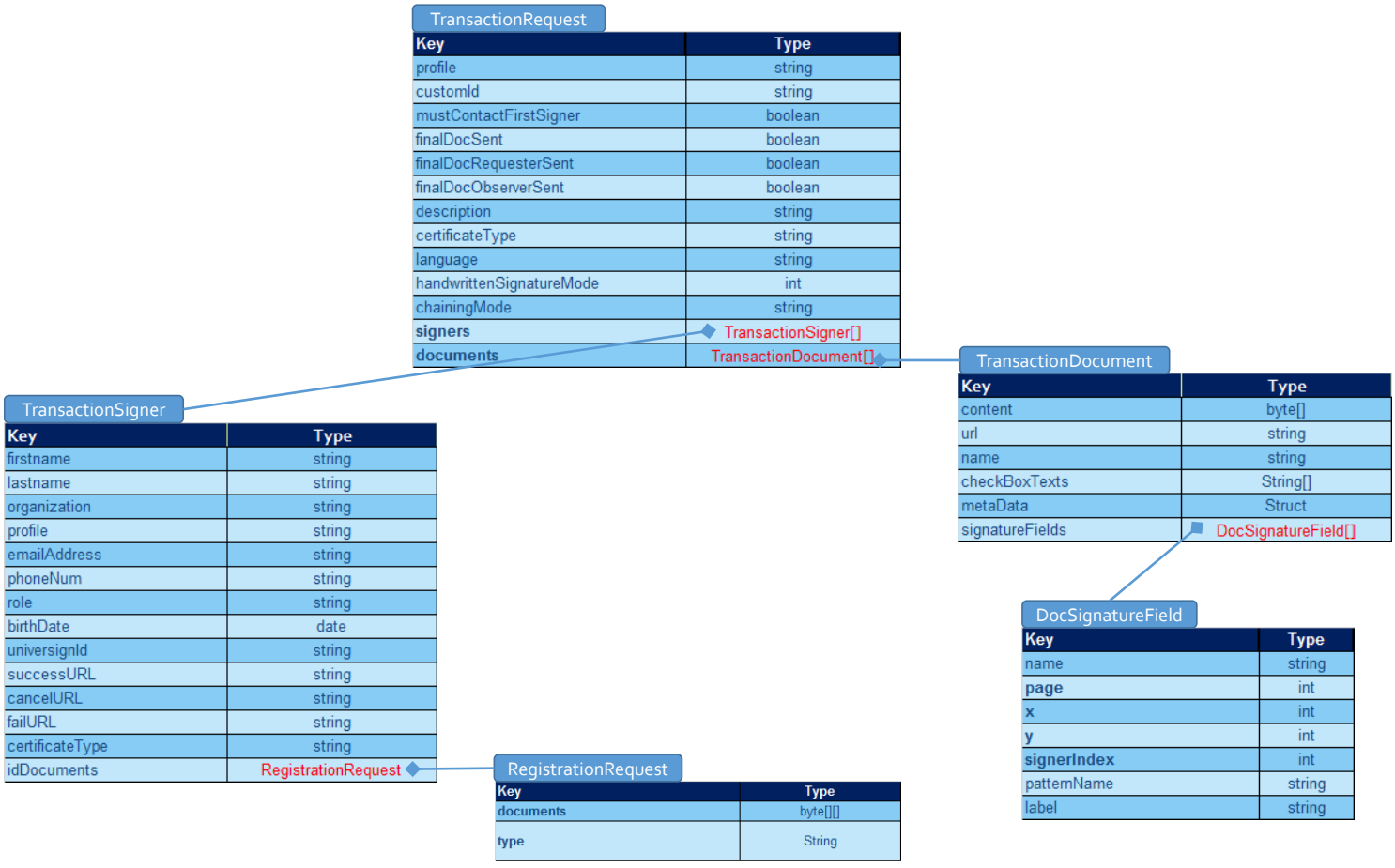
5.2 Prérequis

La création d'une collecte doit obéir à certains prérequis :

- Pour les signataires :
  - Chaque signataire doit posséder un email et un numéro de mobile valide.
- Pour les documents :
  - Les documents à signer sont au format PDF uniquement
  - Chaque document PDF ne doit pas excéder 10 Mo.
  - L'ensemble de documents PDF ne doit pas excéder 15 Mo.

5.3 Structures composant une collecte de signature

Le diagramme ci-dessous représente les structures composant une collecte.



Le tableau ci-dessous indique les méthodes et structures à utiliser en fonction des actions à effectuer.

Action	Méthode utilisée	Structure associée	Données d'entrée / Données en sortie
Créer une collecte de signature	RequestTransaction	TransactionRequest	Entrée
Déclarer des signataires	RequestTransaction	TransactionSigner	Entrée
Déclarer des signataires pour signature certifiée	RequestTransaction	TransactionSigner + RegistrationRequest	Entrée
Déclarer les documents à signer	RequestTransaction	TransactionDocument	Entrée
Définir l'emplacement du cartouche de signature	RequestTransaction	DocSignatureField	Entrée
Déclarer des URLs de redirection en fin de collecte	RequestTransaction	TransactionSigner	Entrée
Connaître l'état d'avancement d'une collecte	getTransactionInfo		Sortie
Récupérer les documents signés	getDocuments		Sortie

Dans la suite du document, nous verrons comment déclarer l'ensemble de ces structures.

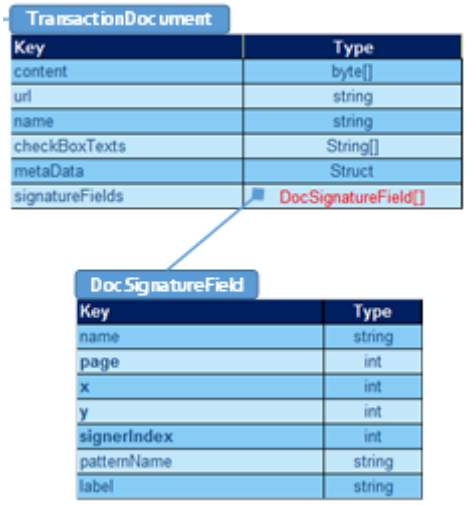
5.4 Déclaration des documents à signer

Pour créer un nouveau PDF dans une collecte de signature, il est nécessaire de :

- Charger le contenu du PDF dans l'attribut **content** ou indiquer son **url**.
- Spécifier le nom du document dans l'attribut **name**.
- Spécifier le tableau de cartouche de signatures utilisé dans le document.

5.4.1 Méthodes utilisées

La déclaration des cartouches de signature s'effectue en déclarant la structure « ***DocSignatureField*** », cette structure hérite de la structure « ***SignatureField*** ».

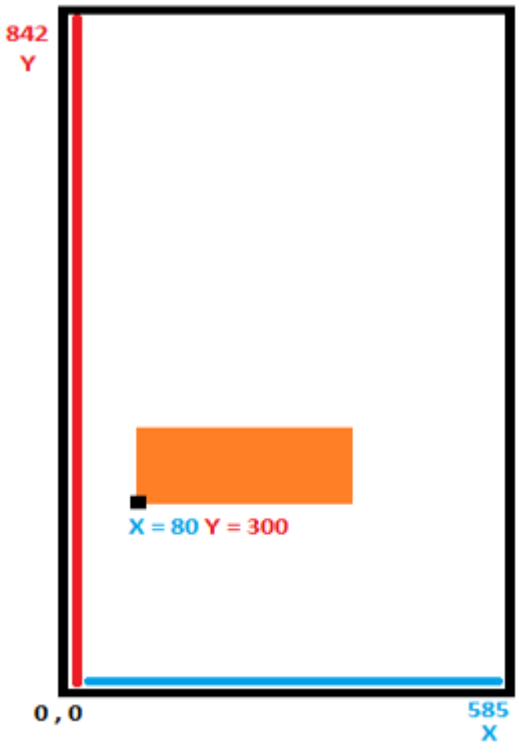


5.4.2 Déclaration des cartouches de signatures

➢ *Emplacement des cartouches de signature*

Le cartouche de signature est la représentation graphique liée à une signature électronique sur un document PDF. Dans le cadre de la signature électronique Universign, ces objets sont identifiés par le numéro de la page du PDF et des coordonnées en X et Y.

Dans le cas classique d'un document de type PDF au format A4 en mode portrait, la largeur est de 595 et la hauteur de 842. Ces coordonnées sont exprimées dans un repère virtuel comme suit :



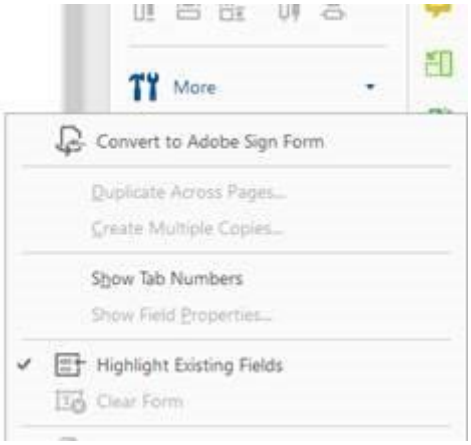
La position du cartouche est identifiée par les coordonnées X et Y partant du coin inférieur gauche du cartouche de signature.

➢ *Utilisation des champs nommés Adobe pour positionner le cartouche de signature*

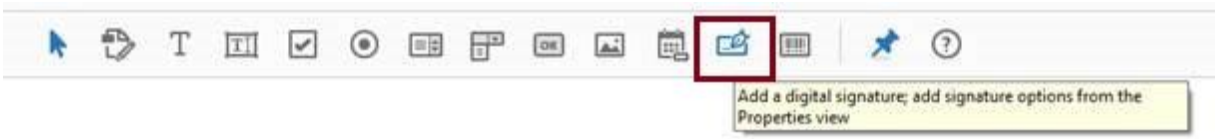
L'API permet de positionner le cartouche de signature dans un champ nommé d'Adobe.

Pour créer une entité nommée sur Adobe, il vous faut l'outil "Préparer le formulaire" (prepare form). Par défaut, un fichier PDF va s'ouvrir avec les options suivantes :

Pour pouvoir éditer un champ de signature digitale, il faut d'abord convertir le fichier en cliquant sur **More** puis **Convert to Adobe sign form**.



La barre de menu affiche désormais l'option de signature digitale.



Vous pouvez alors créer le cartouche de signature et le positionner sur le PDF. Vous reprendrez le nom de ce champ pour l'attribut **name** dans la méthode « ***DocSignatureField*** » (voir ci-après).

➢ *Déclaration des cartouches de signature*

Ci-dessous, les champs de la structure « ***DocSignatureField*** » :

Attribut	Type	Requis	Désignation
name	string	Non	Nom du champ de signature déjà présent dans le document : lors de la signature, ce champ sera remplacé par le cartouche de signature. Si le nom est renseigné, la page, et les coordonnées x et y deviennent alors optionnels. Le cartouche de signature existant doit avoir la même taille que le cartouche de signature électronique. Si le champ correspondant au name n'est pas trouvé dans le document PDF, alors, les attributs **x**, **y** et **page** sont obligatoires
page	int	**Oui**	Numéro de la page du document qui commence à 1. La valeur -1 correspond à la dernière page.
x	int	**Oui**	Coordonnées x du champ de signature dans une page, valant de 0 à 595 pour une page A4 en portrait. Si aucune valeur n'est saisie, la valeur 0 est attribuée par défaut.
y	int	**Oui**	Coordonnées y du champ de signature dans une page, valant de 0 à 842 pour une page A4 en portrait. Si aucune valeur n'est saisie, la valeur 0 est attribuée par défaut.

Attribut	Type	Requis	Désignation
signerIndex	int	**Oui**	Index du signataire de la collecte, le 1er signataire porte l'index 0.
patternName	string	Non	Libellé correspondant au cartouche de signature personnalisé. Universign propose un cartouche par défaut nommé « default », en l'absence de valeur, le cartouche «default » est utilisé.
label	string	Non	Intitulé de la signature du document.

Le numéro de page, les coordonnées en X, Y et l'index du signataire sont des **attributs obligatoires**. Ces attributs font le lien entre le cartouche de signature et le signataire.

5.4.3 Déclaration des documents

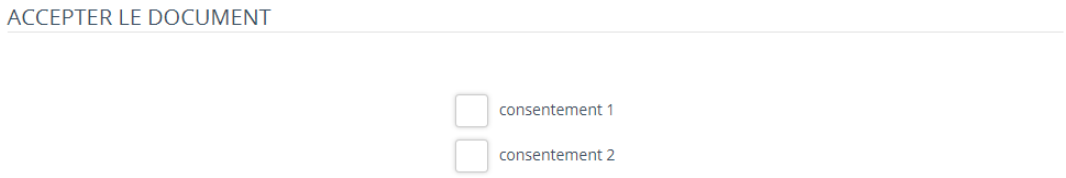
Après avoir défini les cartouches de signatures, il est nécessaire de déclarer les documents PDF puis de rattacher les cartouches de signatures aux PDFs concernés.

Pour déclarer un document, il suffit de déclarer la structure « ***TransactionDocument*** » avec les attributs ci-dessous :

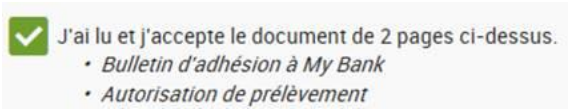
Attribut	Type	Requis	Désignation
content	byte[]	Non	Contenu du document en base 64
url	string	Non	URL de téléchargement du document
name	string	Oui	Nom du document
checkBoxTexts	String[]	Non	Texte des cases de consentement (checkboxes) associées au document
metaData	Struct	Non	Méta données associées au document
signatureFields	DocSignatureField[]	Non	Cartouche de signature du document
documentType	string	Non	Type du document. Les valeurs valides sont : • pdf : la valeur par défaut. • pdf-for-presentation : Cette valeur apposera uniquement un vu sur le document. • pdf-facultatif : Ce type de document PDF peut être refusé et n'être signé par aucun signataire sans annuler la transaction. • sepa : En utilisant cette valeur, aucun document PDF n'est fourni, mais UNIVERSIGN crée un mandat SEPA à partir des données envoyées dans SEPAData.
title	string	Non	Titre du document à afficher

- *CheckBoxTexts*

Il est possible en renseignant le champ « *checkBoxTexts* » de personnaliser des cases de consentement à cocher par document. Il suffit d'envoyer dans ce champ, une liste de chaine de caractères. Cette liste se substituera à la liste statique définie dans le profil de signature.



Attention : en plus de vos checkboxes personnalisées, ajoutez une dernière checkbox vide. Cette dernière checkbox permet de renseigner des labels comme dans l'exemple ci-dessous.



- *MetaData*

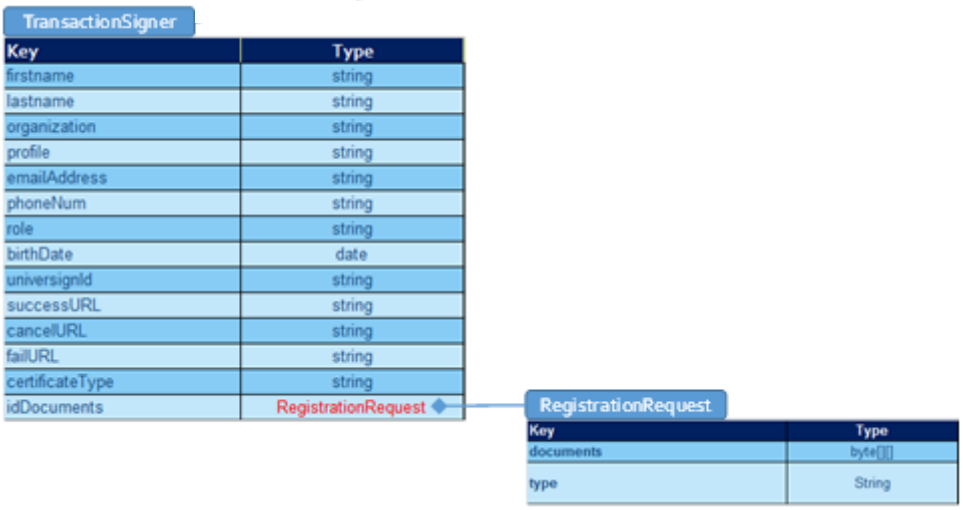
Il est possible d'associer au document une structure de données. Ces métadonnées liées au document seront restituées via l'API avec le document après la session de signature.

5.5 Déclaration des signataires

La déclaration des signataires permet de transmettre :

- Les informations sur l'identité des signataires
- Le niveau de signature requis pour chacun des signataires
- Les coordonnées de chaque signataire
- Les URLs de redirection.

5.5.1 Les méthodes utilisées



Pour déclarer les signataires, il est nécessaire de déclarer la structure « ***TransactionSigner*** ».

Attribut	Type	Requis	Description &Commentaire
firstname	string	Non	Prénom du signataire : requis pour la création d'un certificat de personne physique.
lastname	string	Non	Nom du signataire : requis pour la création d'un certificat de personne physique.
organization	string	Non	Organisation Universign
emailAddress	string	Non	Email du signataire
phoneNum	string	Non	Numéro de téléphone mobile pour la réception du code OTP (One-Time Password) par SMS, s'il n'est pas renseigné, il sera demandé lors de la signature.
birthDate	date	Non	Date de naissance
universignId	string	Non	Un identifiant externe donné par l'organisation qui identifie le signataire.
profile	string	Non	Le nom du profil de signature à utiliser afin de personnaliser la session de signature par signataire (*default* par défaut). Cette personnalisation est mise en place par l'équipe Universign.
role	string	Non	Rôle de l'acteur de la signature (*signer* par défaut) : Le **signataire** est en mesure d'afficher les documents et de les signer. L'**observateur** (*observer*) n'intervient que pour suivre la collecte et afficher les documents à signer et signés
successURL	string	Non	URL de redirection vers laquelle le signataire sera redirigé suite à la session de signatures terminée avec succès.
cancelURL	string	Non	URL de redirection vers laquelle le signataire sera redirigé suite à la session de signatures annulé. La valeur par défaut est "*successURL*".
failURL	string	Non	URL de redicrection vers laquelle le signataire sera redirigé suite à la session de signatures échoué (erreur technique) La valeur par défaut est "*successURL*".

Attribut	Type	Requis	Description &Commentaire
certificateType	string	Non	Indique quel type de certificat qui sera utilisé pour effectuer la signature et donc le type de signature effectuée par ce signataire. Les valeurs possibles sont : ***simple*** : permet aux signataires d'effectuer une simple signature (valeur par défaut). ***certified*** : Permet aux signataires d'effectuer une signature certifiée (niveau 2). ***advanced*** : Permet signataires d'effectuer une signature électronique avancée (niveau 3) qui exige les mêmes options qu'une signature certifiée. Ce cas n'est pas traité dans le présent guide.
idDocuments	**Registration Request**	Non	Les documents d'identité à utiliser pour l'enregistrement du signataire. Si cette option est activée, l'utilisateur ne sera pas invité à fournir ses documents d'identité dans le workflow de signature.

Les signataires doivent être déclarés dans un tableau ordonné.

Un signataire est identifié par son index dans ce tableau ordonné, **l'index commence à zéro**.

Tous les attributs sont optionnels, mais certains attributs sont nécessaires suivant le scenario de signature.

5.5.2 Identité des signataires

Un signataire est désigné par les paramètres suivants :

- firstname : prénom du signataire
- lastname : nom du signataire
- emailAddress : email du signataire
- phoneNum : numéro de mobile
- birthDate : date de naissance

Ces paramètres sont facultatifs, mais l'adresse mail est obligatoire pour le 1er signataire si l'invitation à signer génère un email.

Si le scenario comporte la création ou l'utilisation d'un **certificat certifié** ou **qualifié**, il faudra alors renseigner obligatoirement les champs suivants :

- Firstname,
- Lastname,
- PhoneNum.

5.5.3 Déclaration des options de signature

Le niveau de signature est défini par le paramètre certificateType :

- *simple* pour une signature de niveau 1 (valeur par défaut)

- *certified* pour une signature de niveau 2
- *advanced* pour une signature de niveau 3

5.5.4 Les URLs de retour

Les URLs de retours permettent de rediriger le signataire suite à sa signature. 3 cas sont prévus :

1. **URL success** :
   URL vers laquelle le signataire sera redirigé suite à la session de signature terminée avec succès.
2. **URL cancel** :
   URL vers laquelle le signataire sera redirigé suite à la session de signatures annulée. La valeur par défaut est " URLs success".
3. **URL failed** :
   URL vers laquelle le signataire sera redirigé suite à la session de signatures échouée (erreur technique). La valeur par défaut est "URL cancel".

Ces URLs sont paramétrées dans la méthode TransactionSigner.

5.6 Création de la requête de signature

Dans les chapitres précédents, nous avons défini :

- Le tableau des signataires.
- Les cartouches de signatures.
- Les documents à signer.

Il faut maintenant créer la requête de signature en déclarant la structure « TransactionRequest ».

Les attributs de la structure « ***TransactionRequest*** sont les suivants :

Attribut	Type	Requis	valeur par défaut	Désignation
profile	string	Non	default	Nom du profil de signature à utiliser. Les profils de signature sont mis en place par l'équipe Universign. La valeur par défaut est "default".
customId	string	Non		Identifiant unique qui peut être utilisé pour identifier la transaction. Si cette Id n'est pas unique, une exception sera levée. Notez qu'Universign génère son propre identifiant unique pour chaque transaction et le retourne au demandeur
mustContactFirstSigner	boolean	Non	false	Si la valeur est True, le premier signataire recevra une invitation à signer le document (s) par e-mail dès que la transaction est demandée.
finalDocRequesterSent	boolean	Non	false	Indique si le demandeur doit recevoir les documents signés par email lorsque la transaction est terminée.

Attribut	Type	Requis	valeur par défaut	Désignation
finalDocSent	boolean	Non	false	Indique si chaque signataire doit recevoir les documents signés par email lorsque la transaction est terminée.
finalDocObserverSent	boolean	Non	true	Indique si les observateurs reçoivent les documents signés par email lorsque la transaction est terminée.
description	string	Non		Description textuelle des meta donnés de la collecte
certificateType	string	Non	simple	Type et niveau de certificat : simple, certified, advanced
language	string	Non	en	Langue d'affichage parmi : bg ca (Catalan), de, en, es, fr, it, nl, pl, pt, ro.
handwrittenSignatureMode	int	Non	1	Mode de signature manuscrite. 0 : pas de signature manuscrite 1 : signature manuscrite 2 : signature manuscrite si le signataire utilise une interface tactile
chainingMode	string	Non	none	Transition entre les signataires : none, email, web
signers	**transactionsigner**	**Oui**		Tableau des signataires de la transaction
documents	**TransactionDocument**	**Oui**		Documents à signer

Cette structure sera utilisée dans la méthode ***requestTransaction*** pour faire appel au service de signature électronique Universign et créer une nouvelle collecte de signature. L'appel à la méthode ***requestTransaction*** génère une transaction de signature, envoie les documents à signer ainsi que les options de signature, notamment le niveau de signature souhaité. La transaction a une durée de validation de 14 jours à compter de son initialisation.

L'appel à la méthode requestTransaction renvoie une url de signature pour le signataire du type :

https://app.universign.com/sig/#/sign/xxxxx où xxxxx est l'ID du signataire.

5.7 Personnalisation d'un parcours de signature

Universign offre une personnalisation du parcours de signature. Cette personnalisation est optionnelle. Les éléments de personnalisation sont paramétrés par les équipes d'Universign, à partir du cahier de paramétrage que vous avez complété. Les éléments personnalisables sont :

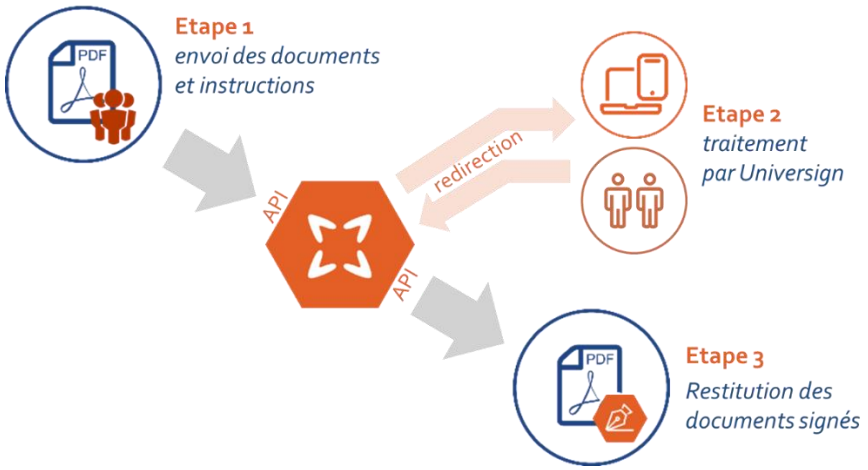
- Les emails de notification
- L'ajout d'un logo sur la page de signature
- Le sms

6 Etat d'avancement d'une collecte

6.1 Introduction

Avant de récupérer les documents signés, il est nécessaire de connaitre l'état de la collecte. Si cette dernière est terminée avec succès (collecte complète), il est alors possible de récupérer les documents signés.

Les API Universign mises à disposition permettent de suivre l'avancement des collectes de signature.



Il existe deux méthodes pour connaître l'état de l'avancement d'une collecte suite à l'envoi d'une requête de signature :

- Les méthodes « ***getTransactionInfo*** » et « ***getTransactionInfoByCustomId*** » interrogeant les serveurs Universign,
- Le mécanisme de callback.

6.2 Retour de la requête de création de collecte.

En retour de la création de collecte, Universign renvoie la structure « ***TransactionResponse*** » contenant les éléments suivants :

Attribut	Type	Désignation
url	string	URL de l'interface WEB pour le premier signataire.
id	string	Id de la transaction

L'id de la transaction peut être utilisé pour connaitre l'état de la collecte de signature et pour récupérer les documents lorsque la session de signature est terminée.

6.3 Requêtes sur l'état d'avancement d'une collecte

Il est intéressant de suivre l'état d'avancement d'une collecte de signature pour effectuer des actions en conséquence : relance des signataires, récupération des documents signés en GED, etc.

6.3.1 GetTransactionInfo

La méthode ***getTransactionInfo*** permet de connaître le statut d'une transaction à partir de son ID Universign.

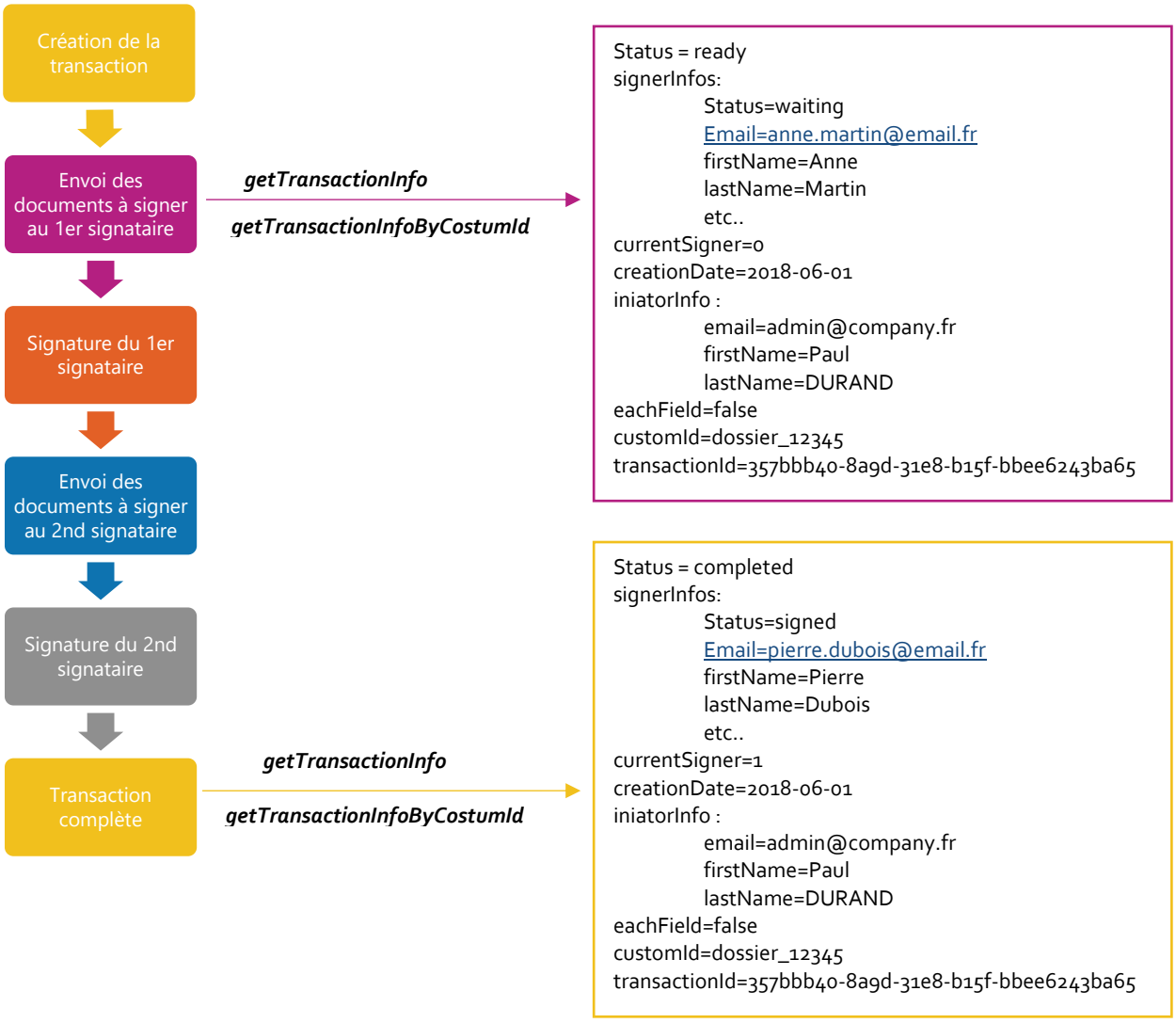
Le résultat de la méthode est une structure ***TransactionInfo*** qui contient les valeurs suivantes :

Attribut	Type	Désignation
status	string	Statut de la transaction parmi : ready / expired / canceled / failed / completed
signerInfos	SignerInfo	Informations relatives aux signataires
currentSigner	int	Index du signataire en cours, le 1er signataire possède l'index 0
creationDate	date	Date de création
description	string	Description de la transaction
iniatorInfo	InitiatorInfo	Informations relatives au créateur de la transaction
eachField	boolean	Information relative à la signature manuscrite
customId	string	ID client de la transaction
transactionId	string	ID Universign de la transaction

6.3.2 GetTransactionInfoByCustomId

Cette méthode est très similaire à la précédente, elle renvoie le statut d'une transaction dans la structure ***TransactionInfo*** à partir du CustomID que vous avez défini. Cette méthode est utilisée dans le cas où vous ne souhaitez pas stocker d'ID Universign.

L'exemple ci-dessous montre le résultat des appels aux méthodes ***getTransactionInfo*** et ***getTransactionInfoByCostumId*** à plusieurs étapes du processus de signature dans le cas d'une transaction complétée par 2 signataires.

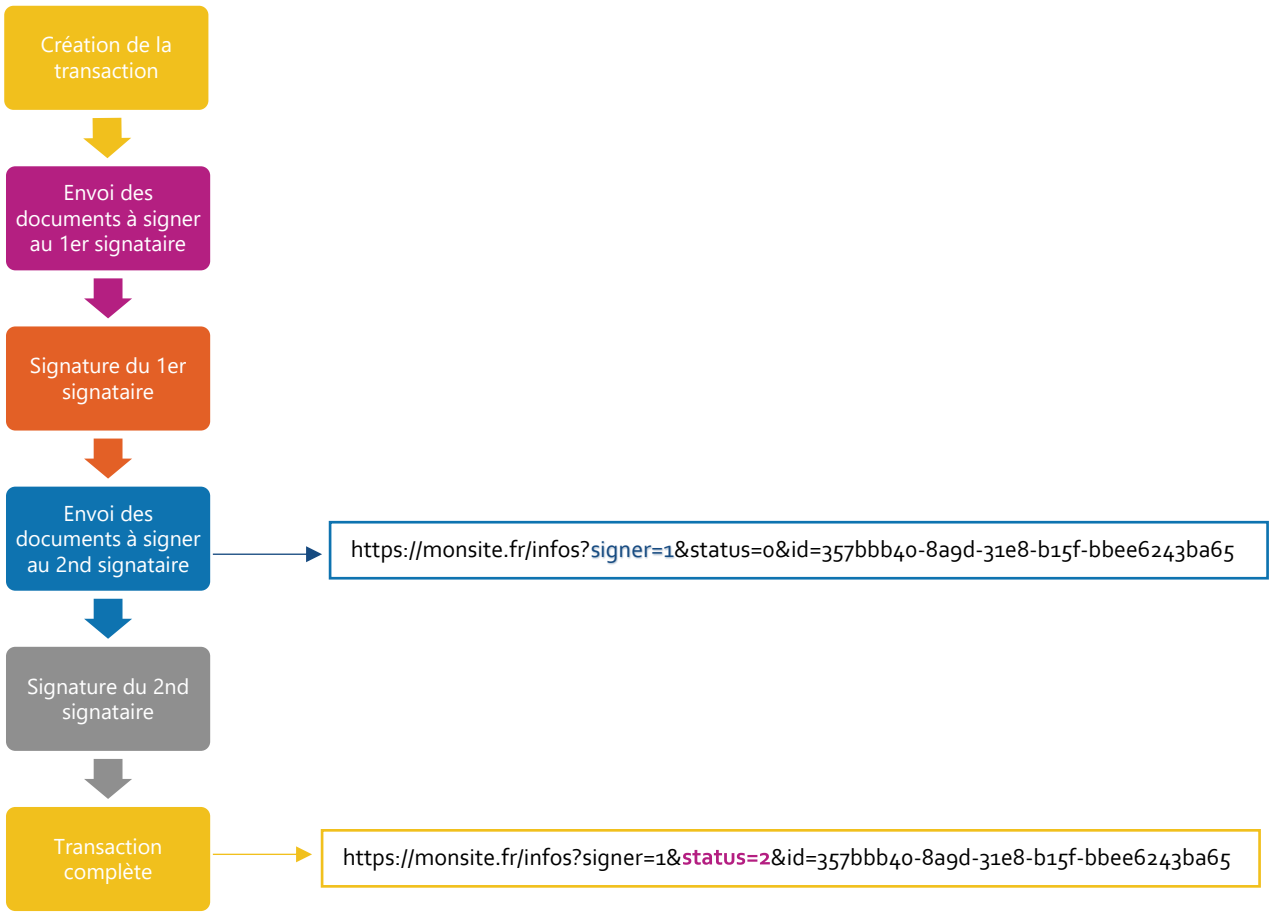


6.4 Les Callback

Les callbacks permettent de connaître le statut de la session de signature en temps réel.

A chaque action ou changement de statut de la session de signature, les serveurs Universign appellent une URL de callback (configurable) dans laquelle des paramètres sont transmis, permettant de connaître l'ID de la transaction, le signataire en cours, le statut de la transaction. L'URL de callback est à transmettre à votre interlocuteur Universign en début de projet.

L'exemple ci-dessous décrit l'évolution du callback au fur et à mesure de l'avancée de la transaction qui est signée par 2 personnes.



Les informations envoyées lors de l'appel au callback sont les suivantes :

- **id** : L'id unique de la transaction
- **Signataire** : L'index du signataire en cours sur la transaction. Cet index commence à 0.
- **statut** : Le statut de la transaction, ce statut peut prendre les valeurs suivantes :
  - 0 : prêt (en attente du prochain signataire),
  - 1 : expiré (collecte créée mais non terminée après 14 jours),
  - 2 : session complétée terminée (tous les signataires ont signé),
  - 3 : annulation de la session par un signataire,
  - 4 : échec (technique) de la session de signature,
  - 5 : en attente de validation par l'autorité d'inscription d'Universign (les signataires ont signé mais les pièces d'identité sont en cours de vérification afin d'établir une identité numérique)

L'URL renvoyée est structurée comme suit :

<url de callback>?signer=[index du signataire]&status=[statut du signataire]&id=[Id de la collecte]

Ce mécanisme permet à un système externe d'être notifié d'un changement de statut, dès l'envoi de la transaction au premier signataire. A réception du l'url sur votre serveur, celui-ci renvoie le code 200 si l'url est bien prise en compte. Dans le cas contraire, tant que l'url de callback n'est pas prise en

compte, la notification est renvoyée toutes les heures pendant 12 heures (pendant 72 heures dans le cas d'une transaction expirée).

7 La récupération des documents signés

7.1 Méthodes utilisées

Lorsque la session de signatures est terminée (la transaction est dite complète), il est possible de télécharger les documents signés via les deux méthodes suivantes :

- ***getDocuments***

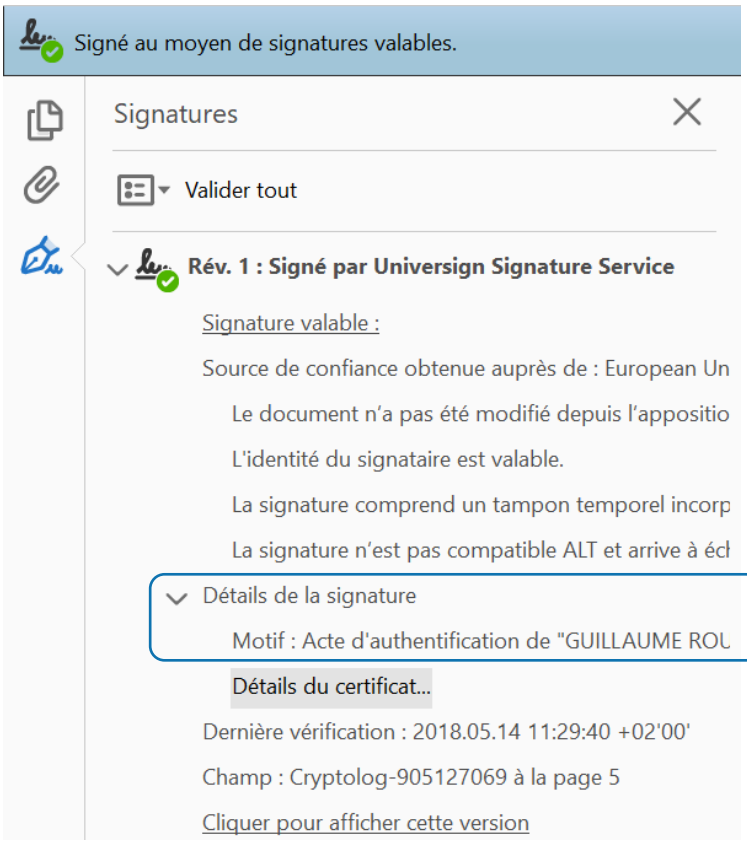
  Cette méthode synchrone permet via l'ID de transaction de récupérer un tableau nommé ***TransactionDocument***. Chaque ligne du tableau correspond à un document signé.

- ***getDocumentsByCustomId***

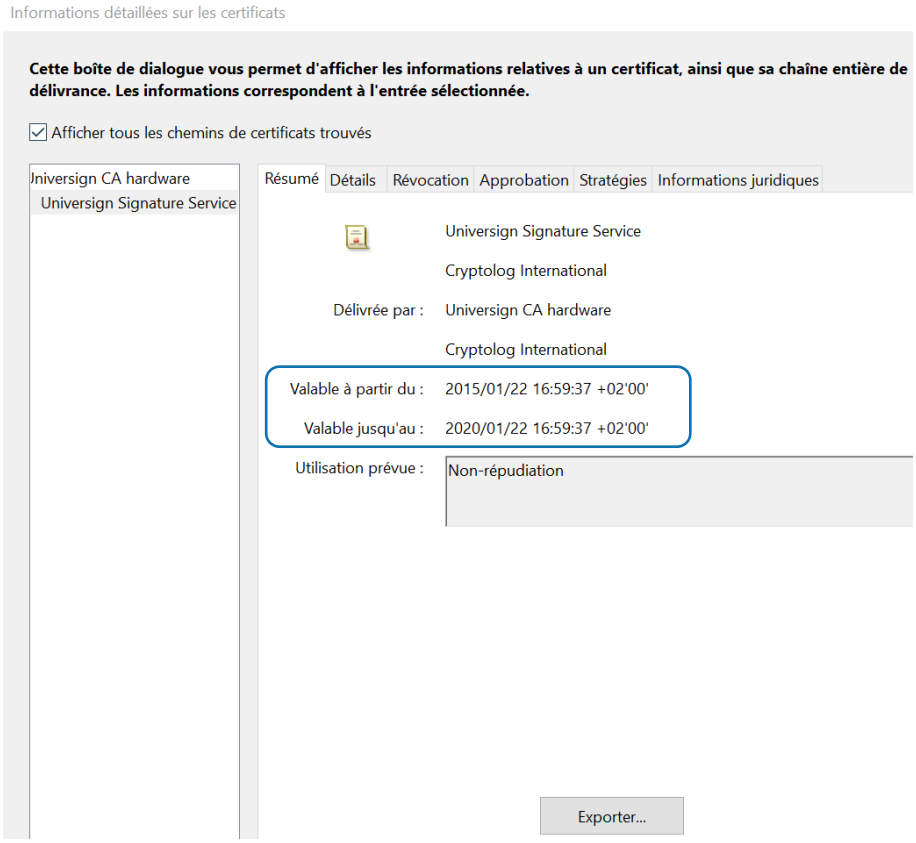
  Cette méthode est équivalente à la première, mais se base sur le ***CustomId*** renseigné par l'utilisateur du service lors de la création de la collecte.

7.2 Vérification des signatures dans un document

Lorsqu'un document PDF est signé électroniquement, les signatures sont contenues dans le fichier. Il est possible d'en vérifier leur validité.



Cliquer sur ***détails du certificat*** permet d'obtenir les informations relatives au certificat : validité, chaque certificat émis est valable 5 ans, autorité certificatrice, révocation, approbation, etc.



8 Cas d'usage de la signature simple

Le cas d'usage décrit ci-dessous est le cas le plus simple, rencontré fréquemment. Les méthodes décrites précédemment s'appliquent à l'ensemble des cas traités par la suite, les exemples de code seront détaillés dans un document annexe. Ils peuvent être étendus aux autres cas d'usage.

8.1 Description du scenario

Prenons le cas d'un contrat d'assurance à signer par un client. Le contrat d'assurance est établi au format PDF. Le service Universign est utilisé pour la signature du contrat.

Le site de démonstration http://demo.universign.eu/1/ vous permet de voir un exemple d'intégration de la signature Universign de niveau 1 pour un document.

Contexte :

- **Type de document** : contrat d'assurance
- Niveau de signature : simple
- **Intégration** : Redirection Universign

Scénario suivi :

- **1 document à signer** : Contrat_durand.pdf
- **1 signataire** : Pierre DURAND, pdurand@entreprise1.com
- Options de signature : **signature simple**

8.2 Méthodes et structures utilisées

- Méthode utilisée : RequestTransaction
- Structures associées :
  - TransactionSigner
  - TransationDocument
  - DocSignatureField

8.3 Exemples de code

Les exemples de codes sont détaillés dans le document Annexe.

9 La signature cachet serveur

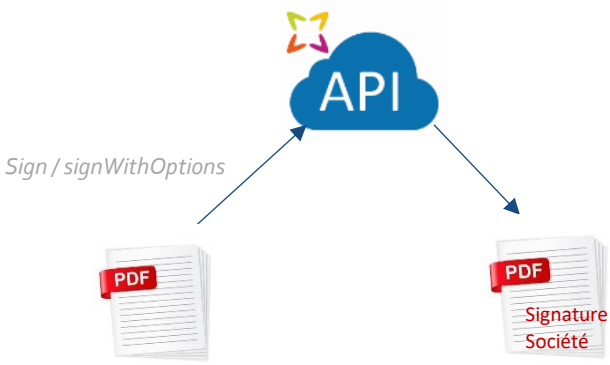
9.1 Introduction

Le cachet serveur est la signature émise par une personne morale, à savoir une entreprise. Pour mettre en place le cachet serveur, nous vous remercions de contacter votre interlocuteur Universign afin de définir les conditions contractuelles et administratives. Le paramétrage du cachet serveur est du ressort de l'équipe Universign.

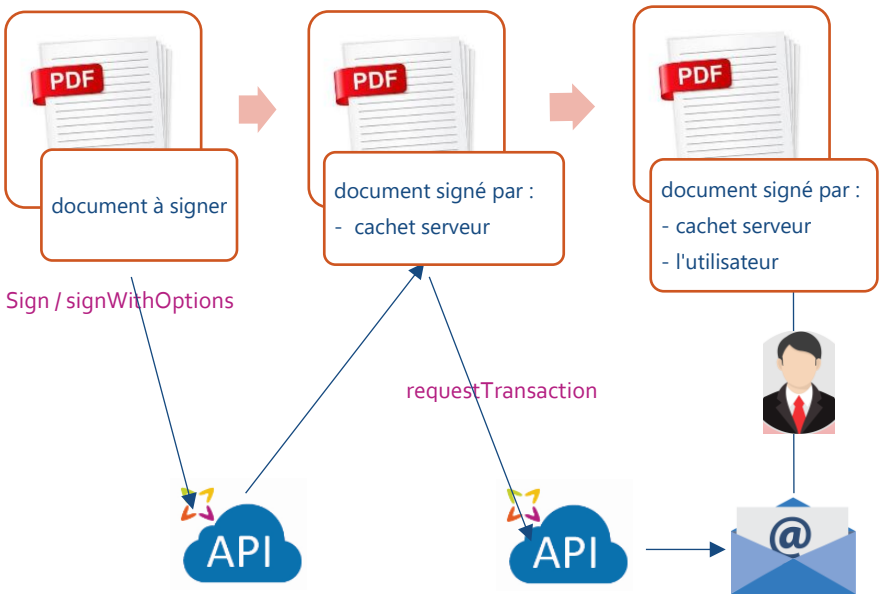
La signature cachet serveur est un mécanisme synchrone. L'apposition d'un cachet serveur sur un document PDF consiste en un appel d'une méthode synchrone. Le retour de cette méthode est le document signé par le cachet serveur.

L'implémentation du cachet serveur peut de faire à plusieurs niveaux :

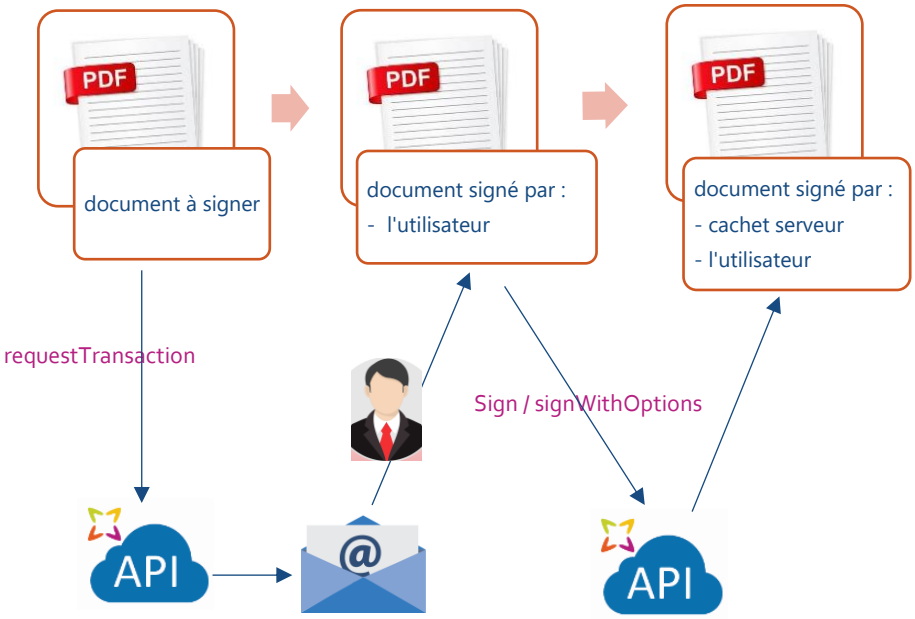
- **Signature d'un document par une personne morale**



- **Cachet serveur en début de transaction : signature d'un document par une personne morale puis signature par une ou plusieurs personnes physiques**



- **Cachet serveur en fin de transaction : signature par une ou plusieurs personnes physiques puis signature d'un document par une personne morale**



9.2 Procédure pour mettre en place le cachet serveur

La mise en place du cachet serveur passe par 2 étapes :

- Administrative : Pour demander un certificat de personne morale pour l'organisation concernée, cette étape requiert la transmission de documents administratifs et justificatifs des statuts d'une organisation :
  - Numéro de SIREN
  - Extrait Kbis de moins de 3 mois
  - Formulaires de demande de Certificat de Personne Morale
  - Signature du mandataire possédant une identité numérique de niveau 2 au minimum
- Technique : Création du cachet serveur côté Universign et paramétrage du cartouche de signature côté client.

9.3 Méthodes utilisées

9.3.1 Méthode sign

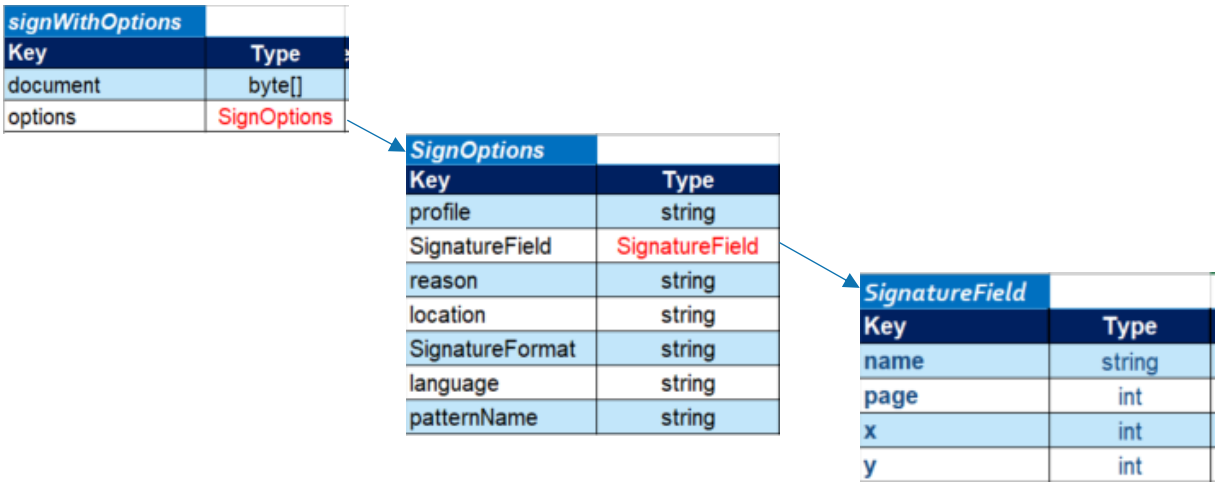
La méthode ***sign*** est le moyen le plus simple pour apposer un cachet serveur sur un document. Cette méthode prend en paramètre d'entrée, le contenu du document en base64 et retourne le document signé avec le cachet serveur.

Key	Type
Document	Byte []

Le document retourné est signé, mais aucun cachet de signature n'est apposé dans le document de manière visible.

9.3.2 Méthode signWithOptions

Dans le cadre de la signature cachet serveur, si le document doit contenir un cartouche de signature, il est nécessaire d'utiliser la méthode « ***signWithOptions*** ».



La méthode « ***signWithOptions*** » prend en plus du document, une structure nommée « ***SignOptions***».

Les attributs de la structure ***SignOptions*** sont :

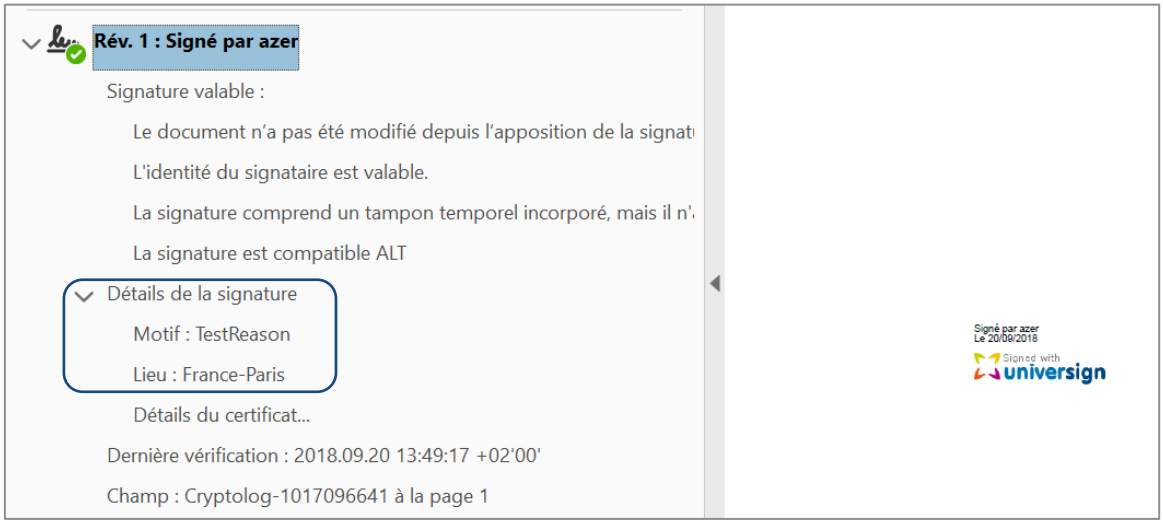
Attribut	Type	Requis	Désignation
profile	string	Non	Nom du profil de signature à utiliser. Les profils de signature sont mis en place par l'équipe Universign. La valeur par défaut est "*default*".
SignatureField	**SignatureField**	Non	Cartouche de signature du document
reason	string	Non	Motif de la signature
location	string	Non	Adresse du poste, de la tablette depuis laquelle la demande de signature est effectuée

Attribut	Type	Requis	Désignation
SignatureFormat	string	Non	Valeurs possibles : - PADES (par défault) - PADES-COMP - ISO-32000-1
language	string	Non	Langue de la transaction valeurs possibles : - en pour l'anglais - fr pour français
patternName	string	Non	Nom du paterne du cartouche de signature (*default* par défaut). Ce pattern est défini au niveau du profil par l'équipe Universign).

Avec cette structure, il est possible de définir :

- Le cartouche de signature du document.
- La personnalisation de ce cartouche.
- Le format de signature.

Les informations contenues dans les paramètres *reason* et *location* font partie de la signature mais ne sont pas affichées dans le cartouche de signature, elles figurent dans le panneau de signatures Adobe.



En retour de la méthode « ***signWithOptions*** », on obtient un tableau de « byte » contenant le document signé.

➢ *Exemple Python*

Cf document Annexe.

10 Cas d'usage du cachet serveur

10.1 Description du scénario

Traitons maintenant la signature d'un contrat de travail par l'employeur (cachet serveur) puis par le salarié. Ce cas est illustré sur notre site de démonstration : http://demo.universign.eu/3/.

Contexte :

- **Type de document** : contrat de travail
- Niveau de signature : simple
- **Intégration** : cachet serveur avec redirection Universign

Scénario suivi :

- **1 document à signer** : contrat_travail_Dupont.pdf
- **1 cachet serveur** en début de transaction
- **1 signataire** : Rose Dupont, rdupont@monmail.com
- Options de signature : **signature simple**

Méthodes et structures associées utilisées :

- RequestTransaction
  - TransactionSigner
  - TransationDocument
  - DocSignatureField
- **SignwithOptions**

Le code associé est détaillé dans le document annexe.

11 Signature certifiée : certificat de personne physique

11.1 Principe

L'émission d'un certificat de personne physique revient à délivrer une identité numérique de niveau 2 ou 3, elle permet d'augmenter la valeur probante d'une signature électronique. Pour plus d'information, vous pouvez consulter l'article correspondant sur la page du support Universign :

https://help.universign.com/hc/fr/articles/115003790485-Pourquoi-et-comment-certifier-mon-identité-sur-Universign-

Universign offre une prise en charge complète de la gestion des identités numériques pour les personnes physiques. Le cycle de vie des identités numériques comprend les étapes suivantes :

- Contrôle des pièces d'identité : Universign intègre un module permettant de valider automatiquement les pièces.
- Création des certificats de signature : Une fois l'identité validée, Universign émet pour la personne un certificat électronique nominatif de signature. Les identités numériques émises par Universign sont reconnues par la loi en France et au niveau Européen. Ces certificats sont réutilisables et mutualisés : une fois émis les certificats permettent de signer sans devoir joindre les pièces d'identité à nouveau.
- Conservation des certificats : Les certificats émis par Universign sont conservés dans notre infrastructure ultra-sécurisée et ne circulent jamais en dehors des serveurs Universign.
- Révocation / Expiration des certificats : Les certificats de personne physique Universign sont valables 5 ans, à la suite de cette durée ils expirent automatiquement. L'utilisateur peut également à tout moment révoquer son certificat.

L'enregistrement d'une personne physique peut intervenir à plusieurs moments de la cinématique de signature :

- **Au cours du processus de signature** :
  Afin de renforcer la valeur probante de la signature, le signataire est invité à enregistrer son identité. Pour cela, le formulaire d'enregistrement de personne physique est complété et les pièces justificatives de son identité (carte nationale d'identité, passeport, etc.) sont transmises. Le signataire remplit le formulaire de demande de certificat et joint les pièces justificatives de son identité.
- **Standalone** :
  Enregistrement d'une demande de certificat pour un utilisateur en mode standalone pour un certificat de niveau 2 : il s'agit d'une demande de certificat de personne physique effectuée en dehors de tout processus de signature.
- **Pré-validation** :
  Le processus de pré-validation est utilisé en amont du processus de signature électronique. La pré-validation a pour objectif de vérifier la correspondance des données d'enregistrement (nom, prénom, date de naissance) d'une personne demandant une identité numérique par rapport aux informations portées sur sa pièce d'identité, ainsi que la qualité des pièces d'identité fournies (format, lisibilité).

11.2 Certification de personne physique en cours de signature

La demande d'enregistrement au cours du processus de signature ne requiert pas d'intégration particulière. Il suffit de déclarer le niveau de signature « certified » dans le paramètre ***certificateType*** dans la méthode ***TransactionSigner***.

L'exemple ci-dessous présente les paramètres à passer dans la structure ***TransactionSigner.***

Key	Values
firstname	Michel
lastname	DUPONT
organization	
profile	default
emailAddress	michel.dupont@domain.com
phoneNum	0615210033
language	fr
role	signer
birthDate	15/01/1950
universignId	
successURL	
cancelURL	
failURL	
certificateType	**certified**
idDocuments	
validationSessionId	

Dans le cas où la demande de certificat est invalidée pour un des signataires, l'ensemble de la transaction est en échec. Pour signer le(s) document(s) à nouveau, il faut générer une nouvelle transaction.

11.3 Certification de personne physique en Standalone

L'émission de certificat en Standalone permet de décomposer le processus de signature certifiée en 2 étapes successives :

- L'enregistrement du certificat du signataire
- La signature du document à proprement dite

L'avantage de l'utilisation du Standalone est que le succès de la transaction ne sera pas conditionné par l'émission du certificat.

L'inconvénient est de scinder cette première signature en 2 étapes distinctes.

Pour les prochaines signatures de niveau 2, l'utilisateur n'aura plus besoin de certifier son identité.

11.3.1 Méthodes utilisées :

La méthode utilisée est **StandaloneRegistration** qui utilise les paramètres de la structure TransactionSigner vue en 5.3.

StandaloneRegistration

Attribut	Type
profile	string
signer	TransactionSigner

TransactionSigner

Key	Type
firstname	string
lastname	string
organization	string
profile	string
emailAddress	string
phoneNum	string
language	string
role	string
birthDate	date
universignId	string
successURL	string
cancelURL	string
failURL	string
certificateType	string
idDocuments	RegistrationRequest
validationSessionId	string

RegistrationRequest

Key	Type
documents	byte[][]
type	String

11.4 Pré-validation

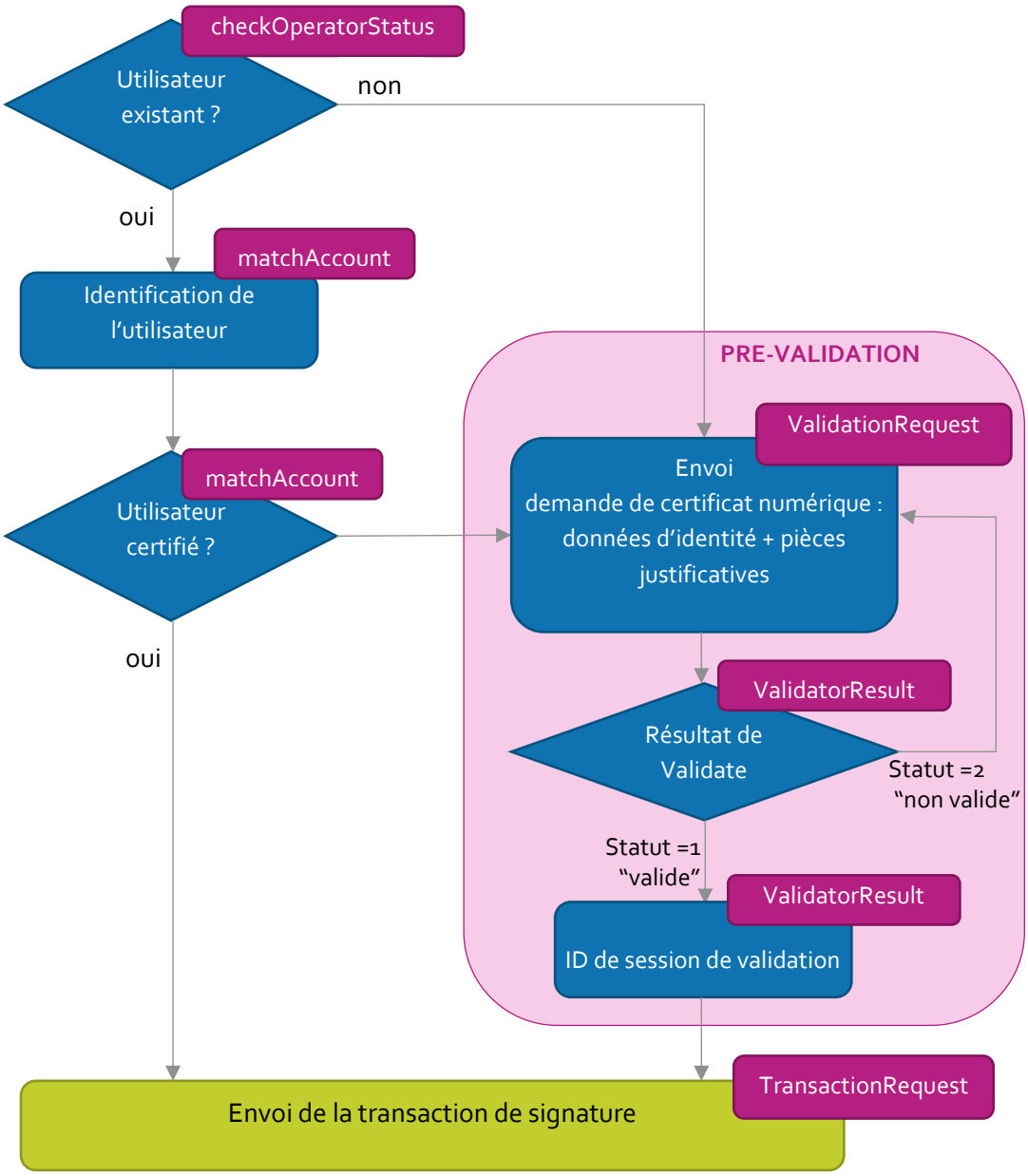
La pré-validation ne permet pas à proprement dit d'émettre un certificat de personne physique, mais de s'assurer que les données d'enregistrement saisies (nom, prénom, date de naissance) sont identiques aux informations portées sur les pièces justificatives d'identité.

La pré-validation est effectuée en amont du processus de signature électronique. Elle permet de garantir l'émission du certificat de personne physique lors de la transaction.

Le logigramme ci-dessous est un exemple d'utilisation de la pré-validation avant de générer une collecte de signature. Dans le processus ci-dessous, les opérations suivantes sont effectuées :

- Vérification de l'existence d'un compte Universign

- Identification de l'utilisateur Universign : information sur la présence d'un certificat d'identité numérique
- Activation du service de pré-validation
- Création de la transaction de signature



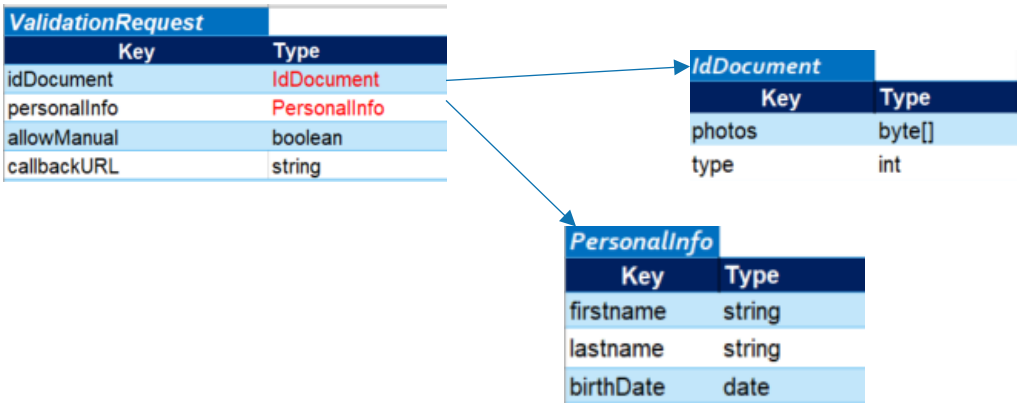
11.4.1 Prérequis

L'activation de la pré-validation est réalisée par les équipes d'Universign. Il est nécessaire de contacter votre interlocuteur Universign ou l'équipe support afin d'activer la pré-validation.

11.4.2 Méthodes utilisées

➢ *ValidationRequest*

Cette méthode permet d'activer les services de validation d'identité Universign : à partir des éléments transmis nom, prénom, date de naissance et documents justificatifs de l'identité.



La structure ***IdDocument*** permet de transmettre les pièces d'identité.

Key	Type	Désignation
photos	byte[]	Liste des documents d'identité à valider
type	int	Type de pièces d'identité: 0 : carte nationale d'identité avec piste MRZ (2 documents attendus : recto et verso) 1 : passeport (1 document attendu) 2 : permis de séjour (2 documents attendus) 3 : permis de conduire Européen avec piste MRZ (2 docs)

La structure ***ValidationRequest*** est détaillée ci-dessous :

Key	Type	Désignation
idDocument	IdDocument	La structure ***IdDocument*** permet de transmettre les pièces d'identité.
personalInfo	PersonalInfo	La structure ***PersonalInfo*** permet de transmettre les informations relatives à l'identité du signataire.
allowManual	boolean	Autorise ou non la validation manuelle des pièces d'identité. Universign recommande de mettre la valeur à false pour forcer la validation automatique.
callbackURL	string	Universign appelle l'URL de callback en y passant les paramètres ID de la session de validation ainsi que son statut, comme dans l'exemple ci-suivant : http://www.company.com/vs?id=123-abc&status=1 Les différents statuts sont : 0 = en cours, 1=valide, 2=invalide

Une transaction de signature ne pourra être logiquement générée que si le statut renvoyé par la méthode ***Validate*** vaut 1.

➢ *MatchAccount*

Le service de Matching est un outil permettant d'identifier un compte existant dans les bases Universign à partir d'un couple Nom/Prénom, ainsi qu'au moins un moyen de contact parmi le couple email /téléphone mobile. La méthode renvoie également l'info sur l'existence d'un certificat (none, advanced, certified). Cette méthode est en général utilisée en amont de la pré-validation puisque dans le cas d'un utilisateur déjà certifié la pré-validation est inutile.

La méthode retourne 2 types de résultats :

- Matching exacte : la méthode détecte un compte qui correspond à 100% aux données saisies. Le compte existe déjà et les coordonnées entrées en input sont les bonnes. Note : seules les données envoyées en input seront affichées en clair. Si l'une des données de contact n'était pas renseignée en input elle sera affichée anonymisée.
- Matching partiel : il existe un ou plusieurs comptes qui sont suffisamment proches des données saisies. La méthode renvoie alors les comptes qui comportent en clair les données qui correspondent exactement et en anonymisées les données à corriger.

Exemple de résultat de la méthode matchAccount exact :

lastname=BERTHIER
firstname=Corinne
mobile=*********19
email=corinne.berthier@universign.com
certificateLevel=certified

Exemple de résultat de la méthode matchAccount partiel :

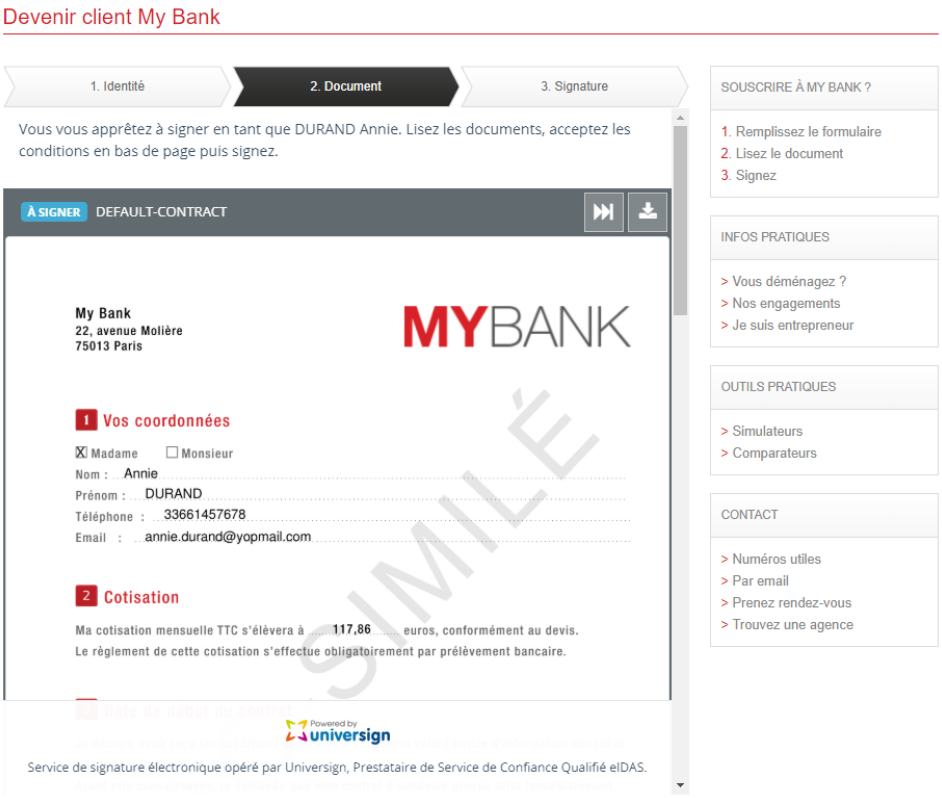
lastname=B**,
firstname=Renaud,
mobile=*********19,
email=m**@h**.**,
certificateLevel=<null>

Paramètre	Type	Requis	Désignation
lastname	string	OUI	Indiquer le nom de naissance ou le nom d'usage. Ce nom doit figurer sur la pièce d'identité qui sera transmise.
firstname	string	OUI	Indiquer le ou les prénoms tels qu'indiqués sur la pièce d'identité qui sera transmise.
mobile	string	NON	Le numéro de mobile devient obligatoire si l'email n'est pas renseigné.
email	string	NON	L'email devient obligatoire si le numéro de mobile n'est pas renseigné.

12 Intégrer la page de signature Universign en mode Iframe

12.1 Utiliser l'Iframe Universign

Il est possible d'intégrer la page de signature Universign en mode Iframe afin de fluidifier votre parcours de signature.



Voici le code à utiliser pour l'intégration de l'Iframe Universign sur votre page web :

```
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <title></title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <script src="https://app.universign.com/sig/embed.js"></script>
  <script>
    function generateIframe() {
    const configuration = {};
    configuration.redirectionMode = 'IN';
    const signerid = '1a5b56a0-6a58-31e8-80b7-c7601f114455';
      /**
       * The universignSigInit function add an iframe element as child of element with
       * id attribute equals to containerId parameter, the attribute src is set from
       * the universignUrl variable, it is the url of the website to be integrated in
       * the iframe, the width and height of the iframe will take 100% of its
       * container.
       *
       * @param {string} containerId The id of the element in which we will inject
       * the iframe.
       * @param {string} signerId The identifier of transaction.
```

```
     * @param {object} configuration The options list to customize the iframe:
     * * redirectionMode {string} This params have two possible values: IN or OUT,
     * the dafault value is OUT,
     * if the value of this params is equal to OUT the redirection will be done
     * outside the iframe (in website container of the iframe),
     * if the value of this params is equal to ÌN the redirection will be done
     * inside the iframe,
     * if the value of this params is otherwise, an exception will be triggered.
     */
    universignSigInit('iframeContainerId', signerid, configuration);
  }
 </script>
</head>
<body onload="generateIframe()">
 <div style="display:flex; justify-content:space-between; align-items:stretch; height:56vh;">
  <div id="iframeContainerId" style="width:70%; display:inline-block; height:auto;">
  </div>
 </div>
</body>
</html>
```

12.2 La nouvelle API Evenement Universign

Vous disposez d'une API événement qui permet d'effectuer le suivi d'une transaction de signature.

Vous pouvez ajouter un "Event Listener" en utilisant 'pdsEvent' qui se déclenche à la creation d'une transaction et à la fin d'une transaction de signature.

Utilisez e.detail.eventType pour connaître l'état de la transaction :

- Begin : la transaction est créée
- End : la transaction est terminée

Utilisez e.detail.signerId pour obtenir le SignerID de la transaction.

Les lignes suivantes sont à utiliser pour obtenir le début et la fin de la transaction de signature.

```
<script type="text/javascript">
  // add an appropriate event listener
  window.addEventListener('pdsEvent', (e) => {
        // e.detail.eventType return 'begin' or 'end' of signature process
        // e.detail.signerId get the Signer Id
  });
</script>
```

NB1. Si vous passez de l'ancienne page de signature Universign à la nouvelle, il est à noter que la redirection était réalisée à l'intérieur de l'Iframe alors que désormais, la redirection se fait à l'extérieur.

NB2.Il est à noter également que l'Iframe Universign permet désormais de rediriger le signataire à l'intérieur de l'iframe ou à l'extérieur.