GUIDE DE DÉMARRAGE DU CACHET SERVEUR UNIVERSIGN

Universign

VERSION : 1	DIFFUSION : *PUBLIQUE*	26/08/2016

Table des Matières

1. Avant-Propos

Pour accéder de manière automatisée à ses services, Universign met à disposition des développeurs des APIs (Application Programming Interface) documentées. Ces interfaces, basées sur des protocoles Web standards, vous permettent d'intégrer très facilement le service « cachet serveur » Universign à vos applications.

2. Documentations Standard

- ## Méthodes d'accès

Le service de signature de contrats en ligne repose sur la notion de collecte de signatures. Une collecte de signatures est composée de documents à faire signer et d'une liste de signataires qui vont apposer leur signature sur ces documents.

Chaque signataire est défini par ses nom et prénom ainsi qu'un numéro de téléphone mobile ou une adresse email afin de recevoir son code secret.

Chaque document - au format PDF - est défini par son nom et son contenu.

Chaque requête de création de collecte doit contenir l'URL où rediriger le signataire après que le processus de signature se soit achevé. Il est possible de spécifier des URL différentes en cas de succès, d'échec ou d'annulation.

Universign offre deux options d'accès à son service de cachet serveur :

- Une API basée sur le protocole XML-RPC
- Une API simple basée sur un envoi de formulaire HTTP avec une requête POST facilement intégrable dans n'importe quel environnement de production.

- ## Paramètres d'authentification

La cinématique d'une collecte basique est la suivante :

Sécurité	SSL
Mode d'authentification	HTTP basic authentification
Identifiants	email et mot de passe

Le certificat et la clé utilisés pour signer sont liés au profile de signature par défaut. Si vous souhaitez utiliser d'autres couples clé/certificat, créez de nouveaux profils de signature en envoyant vos couples clé/certificat.

- ## Accès suivant le procotole XML-RPC

Nos exemples de codes utilisent la librairie "XML-RPC for PHP" disponible à l'adresse http://phpxmlrpc.sourceforge.net.

URL	**https://ws.universign.eu/sign/rpc**
Service	signer
Méthode	*sign ()*

- ## Accès avec l'envoi d'un formulaire HTTP par requête POST

Nos exemples de codes utilisent la librairie "XML-RPC for PHP" disponible à l'adresse http://phpxmlrpc.sourceforge.net

URL: https://ws.universign.eu/sign/post/

Paramètres du formulaire encodés selon le mime-type 'application/multipart-form-data' :

file	le document à signer

Le serveur renvoie le fichier signé.

- ## Exemple de code (en Python)

```
import xmlrpclib;

if __name__ == "__main__":
   pdfDocument = xmlrpclib.Binary(open("myDoc.pdf").read())

   proxy = xmlrpclib.ServerProxy("https://me@myCompany.com:myPwd@ws.universign.eu/sign/rpc")
   signedPdfDocument = proxy.signer.sign(pdfDocument)
   f = open("mySignedDoc.pdf", "w+")
   f.write(signedPdfDocument.data)
   f.close()
```

3. Documentation Avancée

URL	https://ws.universign.eu/sign/rpc
Service	Signer
Méthode	sign()
Paramètre 1	Le document PDF à signer
Paramètre 2	Les options de signature
Retour	Le document signé

Les options de signature sont regroupées sous la forme d'un bean composé des membres suivants :

- profile
- signatureField
- reason
- location
- signatureFormat

profile

Un profil de signature désigne un certificat et une clé privée utilisés pour signer un document. Les profils sont désignés par un nom symbolique, choisi par l'utilisateur ou bien généré automatiquement.

Lors du premier envoi de clé privée, un profil de signature par défaut nommé default est créé. Il est possible par la suite d'ajouter d'autres certificats et clés privées, qui seront liés à autant de profile de signature.

signatureField

Description visuelle de la signature. Cette option permet de spécifier la représentation visuelle de la signature dans le document signé (image, texte, etc.). Si cette option est absente, la signature sera invisible.

reason

La raison de la signature du document.

location

La localisation du signataire.

signatureFormat

Le format de la signature. Les valeurs possibles sont :

- PADES : La signature respecte le format ETSI TS 102 778-3 PAdES Part 3: PAdES Enhanced - PAdES-BES.
- PADES-COMP : La signature respecte le format ISO 32000-1 avec l'attribut signing certificate. Ce format est compatible avec PAdES (même sémantique que PAdES avec le format ISO 32000-1).
- ISO-32000-1 : La valeur par défaut. La signature respecte le format ETSI TS 102 778-2 PAdES Part 2: CMS Profile based on ISO 32000-1.

4. Support & Aide Universign

Le service de signature Universign, disponible 24h/24 et 7j/7, est limité à une signature par seconde.

Lorsqu'une requête échoue, Universign indique un code d'erreur qui vous permet de comprendre et de résoudre le problème rencontré.

- 73002 - une erreur est survenue pendant l'opération de signature.
- 73003 - une erreur est survenue pendant la lecture de votre certificat.
- 73010 - l'authentification a échoué.
- 73011 - aucun compte disponible.
- 73024 - le fichier est illisible.

Ce code et un message d'erreur sont retournés sous la forme d'une exception en XML-RPC, ou sous forme de texte en HTTP.

Lors d'une requête POST, différents codes de réponse HTTP peuvent être renvoyés :

- 400 - requête malformée ou option non supportée.
- 401 - problème d'authentification : utilisateur inconnu ou mot de passe incorrect.
- 403 - problème sur le compte : plus de sceau ou pack expiré.
- 404 - ressource non trouvée, ceci est probablement dû à une erreur d'URL.
- 500 - erreur interne au service Universign. veuillez réessayer plus tard ou contacter le service support.

5. Contactez-nous !

Vous souhaitez intégrer pleinement la solution Universign à votre environnement IT, merci de prendre contact en cliquant-ici