Spécifications Mareva

–

cas des certificats de signature (Version 3 – juillet 2016)

Les certificats de signature :
Douane et Opérateurs EDI (toutes catégories)

4.3.2.Certificats

Un ou deux certificats X509 publics devront être fournis par le prestataire de connexion et insérés dans le référentiel ROSA. La possibilité d'avoir deux certificats permet une transition en douceur pour les changements de certificats : la Douane acceptera les signatures produites par l'un ou l'autre sous réserve d'un délai suffisant (un mois) pour prendre en compte le nouveau certificat.
Réciproquement, la Douane fournira deux certificats X509 publics et la signature douanière pourra être faite indifféremment par l'un ou par l'autre. Lors d'un changement de certificat, la Douane préviendra les prestataires de connexion un mois à l'avance pour leur permettre de réaliser les opérations nécessaires pour accepter la nouvelle signature.
La Douane comme le prestataire de connexion doivent pouvoir accepter des messages signés par au moins un et au plus deux certificats publics.

4.3.2.1.Certificats douaniers

Les certificats douaniers publics de signature sont disponibles sur le site prodouane, rubrique « prestataires EDI ».

4.3.2.2.Certificats Prestataire de Connexion, Editeur de Logiciel et Opérateur EDI client d'Editeur :

Ces certificats doivent être obtenus auprès des autorités de certification agréées par le ministère des finances :

http://www.lsti-certification.fr/images/liste_entreprise/Liste PSCe.pdf

http://references.modernisation.gouv.fr/liste-des-offres-référencées

Les impératifs à respecter pour les certificats à fournir sont cumulatifs :
- certificat délivré par un prestataire qualifié RGS au sens du décret 2012-112,
- certificat à usage de "Cachet" : mention « Cachet » indiquée sur le descriptif,
- certificat conforme à la V2.0 (mention V2,0 indiquée sur le descriptif) (1),
- niveau de sécurité : niveau 1 étoile au minimum,
- certificat commercialisé,
- certificat à destination des Entreprises/Administrations,
- certificat non déqualifié ni révoqué.

(1) les certificats de cachet V1 (dénommés RGS_A_10) sont refusés à compter du 1er juillet 2016, la période transitoire étant terminée.

Ces certificats doivent être fournis à la Douane lors de la création de l'agrément PEDI (phase préalable au test d'interconnexion qui détermine l'envoi du contrat de connexion). Ils sont enregistrés dans la relation PEDI (ROSA) du prestataire de connexion (ou Editeur de Logiciel ou opérateur client d'un Editeur).

Important : Les certificats fournis à la douane doivent toujours être en cours de validité. Avant que la date de fin de validité soit atteinte, ou si le certificat - ou

l'Autorité de Certification- a été déqualifié ou révoqué, le prestataire de connexion EDI (ou l'Editeur de Logiciel ou l'opérateur EDI client d'un Editeur) doit impérativement fournir un nouveau certificat valide à la Douane.

Rappel des engagements souscrits par l'opérateur dans son Contrat de Connexion :

Article 3 : Respect des spécifications techniques

Le bénéficiaire de la connexion s'engage à respecter les spécifications techniques définies par la douane pour l'échange de messages EDI.

Article 7 : Suspension et retrait du contrat

Le contrat de connexion est suspendu ou son bénéfice retiré lorsque les conditions exigées pour son octroi ne sont plus remplies ou lorsque le bénéficiaire n'a pas respecté ses obligations.

4.3.2.2.1 Format du certificat à transmettre

Il y a deux formats d'encodage des certificats:
- le format DER est un format binaire utilisé pour encoder les certificats en notation ASN.1
- le format PEM est du DER encodé en base 64 auquel sont ajoutées des entêtes ASCII.

Le certificat de signature MAREVA doit être transmis à la Douane par le prestataire EDI au format PEM.
L'extension du certificat **n'est pas un indicateur de son format.** Un certificat dont l'extension est *.crt peut être encodé en DER (binaire) ou en PEM (base 64).

Pour connaître l'encodage d'un certificat, utiliser les deux commandes openssl ci-dessous. Si le certificat est au
format DER il s'affichera à l'écran avec la première commande. S'il est au format PEM il s'affichera avec la deuxième commande.

```
openssl x509 -inform DER -in certificat -noout -text
openssl x509 -inform PEM -in certificat -noout -text
```

où `certificat` est le certificat dont on teste le format d'encodage.
L'annexe A présente l'affichage d'un certificat réalisé avec ces commandes.
Pour modifier l'encodage d'un certificat du format DER au format PEM, utiliser la commande :

```
openssl x509 -in certificatDER -inform DER -out certificatPEM -outform PEM
```

où `certificatDER` est le certificat encodé en DER
`certificatPEM` est le certificat encodé en PEM

Note :

Les certificats de signature conformes doivent être envoyés au service Certification-Edi du CID (certification-edi@douane.finances.gouv.fr) avec une extension ".crt" ou ".cer".