# Table des matières

# 1 Généralités

Ce document explique le fonctionnement de la communication TEI entre l'administration fédérale des douanes (AFD) et les partenaires de la douane reliés au NCTS.

La communication est basée sur les standards suivants:

| | |
|---|---|
| **UN/EDIFACT** | United Nations Electronic Data Interchange for Administration, Commerce and Transport. |
| **SMTP** | Transmission des annonces via Internet |

# 2 Transmission par Internet

## 2.1 Principes

Les transmissions via Internet sont plus critiques que celles par X.400 en ce qui concerne la sécurité et la protection des données. Les mesures suivantes tiennent compte de cet aspect:

- Les transmissions **doivent**, pour le moins, **être signées** électroniquement. Par vérification de la signature électronique le destinataire peut contrôler si l'annonce provient effectivement de l'expéditeur mentionné et qu'elle n'a pas été modifiée en cours de route.

- Même avec une signature il est néanmoins possible, non sans difficultés (c.-à-d. avec le know-how correspondant et l'accès aux notes de communication), d'intercepter des données durant la transmission et d'en évaluer le contenu. Si le partenaire de la douane le juge utile, il est possible de coder les données des déclarations transmises en plus de la signature.

- Chaque partenaire de la douane doit désigner une personne de contact responsable de la communication par Internet.

L'Administration fédérale des douanes ne peut garantir le respect de la protection et la sécurité des données que pour les activités, les réseaux, les composants de hardware et de software de son propre domaine d'influence. Elle n'endosse aucune responsabilité quant aux conséquences de l'utilisation abusive de données durant la transmission des données du système TEI du partenaire de la douane à celui de l'administration des douanes et retour.

## 2.2 Signature électronique / codage

Est utilisée la dénommée signature asymétrique resp. la procédure de codage S/MIME. Cette procédure travaille à l'aide d'un couple de codes.

Le code secret (Private Key) est unique, c.-à-d. qu'un seul exemplaire est nécessaire pour le titulaire. Ce Private Key est utilisé pour la génération d'une signature électronique et pour le décodage de données codées. **Il doit impérativement être protégé (tenu secret).**

Le pendant de ce code secret et le code officiel (Public Key). Ce code est en principe accessible à tous et sert au contrôle de l'authenticité d'une signature électronique ou au codage de données.

Le couple de codes évoqué est généré par des instances de confiance (office de certification = CA/Certification Authority). Pour l'application NCTS c'est l'administration fédérale des douanes.

Le couple de codes est transmis par email en format PKCS#12 à la personne de contact responsable de la communication du partenaire de la douane. Le fichier transmis contient, en plus du code privé et public, aussi le code CA officiel de la DGD (self signed).

Le fichier PKCS#12 est lui-même protégé par un mot de passe. Le mot de passe d'accès est adressé au partenaire de la douane par lettre signature afin d'assurer que seul la personne autorisée entre en possession du code.

Pour le NCTS un couple de codes (certificat) séparé par adresse email du partenaire de la douane est établi. Néanmoins celui-ci n'est valable que pour une période restreinte (pour le NCTS une année au minimum, mais au maximum deux ans). 30 jours avant l'échéance du délai de validité, l'ordinateur de la douane établi automatiquement un nouveau certificat (certificat suivant) et le transmet soit à la personne de contact responsable du partenaire de la douane (par email signé) soit de manière analogue aux annonces de déclaration directement au système de production (la différenciation entre l'annonce de déclaration et le certificat suivant se fait sur la base du « Content-Description »: le certificat suivant est désigné « NEW NCTS CERTIFICATES »).

Le certificat suivant peut être utilisé immédiatement après installation. Le système de la douane remplace le certificat actuel par le certificat suivant dès l'arrivée de la première déclaration transmise à l'aide du nouveau certificat. Les déclarations signées/codées avec l'ancien certificat sont traitées telles quel jusqu'à la fin du délai du certificat; mais les réponses sont signées/codées à l'aide du nouveau certificat. D'autre part il est aussi possible que pour un certain temps le système TEI du partenaire de la douane doivent traiter des réponses aux déclarations signées /codées à l'aide de divers certificats, c'est-à-dire que selon la réponse divers certificats seront nécessaires pour le contrôle des signatures resp. pour le décodage des données. Ce problème peut être résolu par le partenaire à l'aide d'un historique des certificats. Une autre possibilité réside dans le fait de n'activer le certificat suivant que lorsque les réponses au déclarations comportant l'ancien certificat sont parvenues au système TEI.

### 2.2.1 Description technique « Signature »

Les annonces traitées et transmises sont signées en S/MIME:

| | |
|---|---|
| Envelope MIME-Attribute | MIME-Version: 1.0<br>Content-Type: multipart/signed; protocol= "application/x-pkcs7-signature"; micalg=sha1 |
| Attachment MIME-Attribute (déclaration, réponse) | Content-Type: application/octet-stream<br>Content-Transfer-Encoding: base64 |
| Attachment MIME-Attribute (signature) | Content-Type: application/x-pkcs7-signature; Name= "smime.p7s"<br>Content-Transfer-Encoding: base64<br>Content-Disposition: attachment; filename="smime.p7s“ |

Chaque annonce signée doit contenir le certificat de l’expéditeur (multipart/signed et application/x-pkcs-signature MIME-Format).

### 2.2.2 Encodage

**Description technique de transmissions signées et codées**

| | |
|---|---|
| Envelope MIME-Attribute | MIME-Version: 1.0<br>Content-Type: application/x-pkcs7-mime; name="smime.p7m"<br>Content-Disposition: attachment; filename="smime.p7m"<br>Content-Transfer-Encoding: base64 |

**Echange de codes pour annonces codées**

Le code officiel du partenaire de communication est utilisé pour l’encodage. Lors de la première attribution des codes la DGD, en tant qu’émetteur des codes, est déjà en possession des codes officiels correspondants du partenaire.

Le code officiel de la DGD est transmis par email signé en tant que certificat au responsable du système du partenaire. Pour autant qu’il ait installé le certificat CA de la DGD (du fichier PKCS#12 transmis auparavant) celui-ci peut contrôler l’exactitude du certificat et ensuite l’installer pour le décodage des annonces de déclaration.

## 2.3 Standards

| | |
|---|---|
| Logiciels utilisés (par l'administration des douanes) | OpenSSL |
| Format du courriel (mail) | MIME 1.0 |
| Format du courriel sécurisé (secure mail) | S/MIME 2 |
| Format du certificat | X509v3 |
| Echange de certificat | PKCS#12 |
| Syntaxe des annonces | PKCS#7 |

## 2.4 Adresses courriel des systèmes de la douane

- Système test:
  - transit@nctstest.ezv.admin.ch
  - autoanswer.transit@nctstest.ezv.admin.ch
- Système de production
  - transit@ncts.ezv.admin.ch
  - autoanswer.transit@ncts.ezv.admin.ch

## 2.5 Traitement des erreurs de déclarations signées ou codées

Lorsqu'une déclaration est correcte du point de vue de la sécurité celle-ci est libérée pour traitement subséquent dans l'application NCTS. Si par contre une annonce ne peut pas être décodée ou vérifiée, la réponse aura la forme d'une DSN « Delivery Status Notification ».

| **Annonces d'erreurs possibles** | **Motif** |
|---|---|
| Decoding failed (5.7.5) | Mauvais certificat de décodage |
| Verification failed (5.7.7) | Motif: annonce signée incorrectement |
| Wrong edi content (5.5.0) | Le contenu du message ne débute pas avec une séquence d'initialisation EDI |
| Smpt_mime_xxx: not allowed/supported for … (5.5.0) | Le niveau de sécurité appliqué ne correspond pas à la configuration (signé/signé et codé) |
| Illegal padding inside the string (5.5.0) | Très vraisemblablement mauvais MIME base64 Encoding |
| Illegal character found in input (5.5.0) | Très vraisemblablement mauvais MIME base64 Encoding |

## 2.6 Scénarii test pour programmateur de logiciel

Avant qu'un programmateur de logiciel effectue des tests avec le système test de la DGD il devrait au préalable effectuer un auto-test en contrôlant si une annonce signée / codée qu'il s'est adressée à lui-même est transmise puis décodée avec succès.

Pour les tests, des certificats test peuvent être demandés auprès de la DGD, ceux-ci sont valables 5 ans.

# 3 Implémentation

## 3.1 Généralités

Cette solution peut être appliquée à toute ou parties de l'application :

- Importation (M90): déclarations et réponses
- Importation (M90): bordereaux des redevances
- Exportation (M90): déclarations et réponses
- Transit und Ausfuhr (NCTS): déclarations et réponses
- Transit (NCTS): DAT et procédure de recherche

Il est donc possible d'utiliser jusqu'à 5 adresses courriel différentes pour communiquer avec le système de l'AFD.

## 3.2 Restrictions

Les déclarations et les réponses NCTS doivent au moins être signées (analogue import et export). Voir point 4.1.

La transmission des DAT ou des fichiers de base s'effectue pour l'instant sans certificat ni codage. Mais il est possible d'utiliser la même adresse que les déclarations et les réponses du NCTS.

# 4 Formulaires de demandes

## 4.1 Formulaire de demande pour exploitation test/production

Le formulaire de demande se trouve sous:

https://www.ezv.admin.ch/ezv/fr/home/declaration-en-douane/declaration-pour-entreprises/ncts---transit-national.html

Le partenaire de la douane doit spécifier notamment:

- Données du transitaire et des déclarants
- Communication : Internet
- DAT : indication de l'adresse email
- Indications générales
- Etc.

De plus, le formulaire de demande contient des directives pour l'exploitation NCTS.

### 4.1.1 Transmission via Internet

Faire remplir, s.v.p., un formulaire de demande séparé par le fournisseur de software. Voir aussi chiffre 4.2 ci-après.

## 4.2 Demande pour transmission de déclarations via Internet

Ce formulaire se trouve sur la page Internet de l'AFD, à l'adresse suivante :

https://www.ezv.admin.ch/ezv/fr/home/declaration-en-douane/declaration-pour-entreprises/ncts---transit-national.html

### 4.2.1 Généralités

Notez en premier lieu si les données suivantes doivent être utilisées pour:

- L'exploitation production
- L'exploitation test
- Ou pour les deux

### 4.2.2 Point 1.1

Données de la personne et de l'entreprise responsable de la configuration Internet du client.

### 4.2.3 Point 1.2

Données du client (partenaire de la douane).

Il est important d'indiquer l'adresse d'envoi des certificats suivants.

### 4.2.4 Point 1.3

Ici, le partenaire de la douane doit indiquer après le transitaire le genre trafic pour lequel les données seront utilisées (importation, exportation, transit).

Lorsqu'un partenaire de la douane travaille avec plusieurs numéros de transitaire mais avec une seule adresse email, celui-ci peut indiquer dans la demande plusieurs numéros de transitaire.