

**SYSTEME D'ECHANGES APPLICATIFS EDI AVEC LA DOUANE
MAREVA
SPÉCIFICATIONS POUR LES PARTENAIRES**

VERSION 1.21 – NOVEMBRE 2013

**DIRECTION GÉNÉRALE DES DOUANES ET DES DROITS INDIRECTS
BUREAU C2 – ARCHITECTURE TECHNIQUE ET DE SÉCURITÉ**



Sommaire

1.INTRODUCTION.....	5
2.OBJET DU DOCUMENT.....	5
3.TERMINOLOGIE.....	5
3.1.OPÉRATEUR.....	5
3.2.PRESTATAIRE DE CONNEXION OU PRESTATAIRE EDI.....	5
3.3.ROSA.....	5
3.4.AGRÈMENT D'INTERCHANGE.....	5
3.5.MESSAGE EDI.....	6
3.5.1.Accusés réception de MAREVA.....	6
3.5.1.1.Exemple d'accusé de réception positif.....	6
3.5.1.2.Exemple d'accusé de réception MAREVA négatif.....	7
3.5.2.Accusés réception du prestataire EDI.....	7
3.5.2.1.Exemple d'accusé réception d'un prestataire de connexion.....	8
3.6.CONSTITUTION D'UN MESSAGE EDI.....	8
3.6.1.Numéro d'enveloppe.....	8
3.6.2.Identifiant de transaction.....	8
3.6.3.Numéro de séquence.....	9
4.PROTOCOLE D'ÉCHANGES MAREVA.....	10
4.1.ADDRESSES DE MESSAGERIE.....	10
4.1.1.Côté Douane.....	10
4.1.2.Côté prestataire de connexion.....	10
4.2.SERVEURS SMTP.....	10
4.3.CONSTITUTION DES MESSAGES.....	10
4.3.1.Pièces jointes.....	10
4.3.2.Certificats.....	11
4.3.2.1.Certificats douaniers.....	11
4.3.2.2.Certificats prestataire de connexion.....	11
4.3.2.2.1.Format du certificat à transmettre.....	11
4.3.2.2.2.Exigences complémentaires.....	12
4.3.3.Constitution du fichier de signature.....	13
4.3.3.1.Quel outil ?.....	13
4.3.3.2.Comment vérifier la signature ?.....	13
4.4.BLOCAGE ET DÉBLOCAGE DU PRESTATAIRE.....	13
4.4.1.Principe.....	13
4.4.2.Format des messages.....	14
4.4.2.1.Message de blocage.....	14
4.4.2.2.Déblocage.....	15
4.5.CONTRÔLES DES MESSAGES ENVOYÉS.....	16
4.5.1.Unicité des messages.....	16
4.5.2.Champs from et to du message.....	16
4.5.3.Horodatage.....	16
5.PROTOCOLE DE TEST.....	16
5.1.APPLICATION DE TEST.....	16
5.2.TESTS.....	16
5.3.VÉRIFICATIONS.....	17
5.4.CONDITIONS DE VALIDATION.....	17
6.CORRESPONDANT MAREVA.....	17

7. TABLEAU DES ERREURS..... 18
ANNEXE A : ELEMENTS POUR LA SIGNATURE ELECTRONIQUE.....32

Modifications apportées

22/12/2006

Paragraphe 1.2.9 Numéro de séquence

Paragraphe 2.4 Horodatage

Juin 2007

Paragraphe 1 Introduction

Paragraphe 1.2.3 Prestataire de connexion

Paragraphe 2.3.2 Pièces jointes

Paragraphe 5.3 Accusé de réception du prestataire de connexion

Paragraphe 8 BLOCAGE et DEBLOCAGE du PRESTATAIRE

Paragraphe 8.1 Principe

Paragraphe 9 Tableau des erreurs

Ajout de l'erreur 55

Novembre 2007

Ajout d'une annexe sur les certificats

Paragraphe 5.3 Accusé de réception du prestataire de connexion

Paragraphe 8 BLOCAGE et DEBLOCAGE du PRESTATAIRE

Paragraphe 8.1 Principe

Dans ces deux paragraphes 5.3 et 8.1 modification du délai de réémission porté de 10 à 20 minutes.

Mars 2010

Restructuration du document (organisation des paragraphes)

Compléments au tableau des erreurs

Mars 2013

Paragraphe 4.3.2.2 Mise à jour référentiel AC

Septembre 2013

Paragraphe 4.3.2.2 Mise à jour exigences certificats + explications supplémentaires chapitre 7

Novembre 2013

Mise à jour du lien Prestataire de services de certification électronique

1.INTRODUCTION

La Douane ouvre un système d'échanges inter-applicatifs avec ses partenaires (mécanismes de type EDI), intitulé MAREVA, acronyme pour Messagerie Applicative en REseau à Valeur Ajoutée.

Ce document décrit le mécanisme MAREVA tel qu'il est vu par les partenaires et spécifie les éléments techniques pour le mettre en œuvre.

Pour pouvoir être mis en œuvre, il nécessite une interconnexion réseau (PASTEUR) entre le partenaire et la Douane, pour pouvoir supporter le protocole réseau utilisé par MAREVA (SMTP). Les spécifications de l'interconnexion PASTEUR font l'objet d'un autre document « Interconnexion sécurisée avec la douane – spécifications pour les partenaires ».

2.OBJET DU DOCUMENT

Ce document présente le dialogue avec le système MAREVA. Il est destiné aux prestataires de connexion.

MAREVA est une messagerie applicative reposant sur les standards suivants:

- SMTP pour le protocole d'échange;
- XML pour le format des documents échangés;
- **SHA1 et RSA pour les mécanismes de signature.**

3.TERMINOLOGIE

3.1.OPÉRATEUR

C'est une entreprise ayant une ou plusieurs relations métier avec la Douane référencées dans ROSA (Référentiel des Opérateurs et du Suivi des Agréments) qui émet des messages fonctionnels vers la Douane.

3.2.PRESTATAIRE DE CONNEXION OU PRESTATAIRE EDI

C'est une entreprise offrant une prestation technique pour assurer l'acheminement des messages fonctionnels d'un opérateur vers la Douane.

Un opérateur peut assurer lui-même cette fonction sans recourir aux services d'un prestataire de connexion. Il est alors lui-même prestataire EDI. Dans ce cas <PartyId> et <ConnexionId> sont identiques (cf ci dessous).

3.3.ROSA

Rosa est un référentiel reprenant les données intrinsèques des entreprises ou individus en relation avec la Douane, et la spécification de ces relations.

MAREVA utilise la relation PEDI pour identifier le prestataire EDI et connaître ses droits à transmettre des messages pour les différents téléservices disponibles.

Le prestataire EDI est identifié par un agrément d'interchange <InterchangeAgreementId> et un son numéro de SIRET <ConnexionId>.

L'opérateur est identifié par son numéro de SIRET <PartyId>.

3.4.AGRÉMENT D'INTERCHANGE

C'est un agrément spécifique du mode EDI attribué aux prestataires de connexion une fois les tests techniques validés. Cette relation ROSA contient en particulier les adresses de messagerie émettrices des messages à destination de la Douane et auxquelles la Douane doit envoyer ses messages techniques et/ou fonctionnels pour les différents téléservices pour lesquels le prestataire EDI est autorisé.

La règle est :

- un agrément par prestataire EDI ;
- une et une seule adresse de messagerie par téléservice. Une même adresse de messagerie ne peut être utilisée pour des téléservices différents.

Si, dans des cas qui doivent rester exceptionnels, des adresses de messagerie différentes sont attribuées pour un prestataire EDI à un même téléservice, il y aura plusieurs agréments donc plusieurs relations PEDI référençant le téléservice.

3.5.MESSAGE EDI

C'est un fichier XML nommé document1.xml.

Il y a trois types de messages dans le système MAREVA :

- message de notification de réussite : message envoyé par le système MAREVA à la douane, dans le cadre de la phase de test avec Diagnostic (module simulant un téléservice douanier), pour valider l'échange réussi de 10 messages successifs avec accusé réception par un prestataire EDI ;
- message fonctionnel : message émis par un prestataire EDI ou par la douane dont le contenu est en relation avec une télé-procédure douanière ;
- message technique : message d'information relatif aux échanges MAREVA.

On distingue :

- les accusés réception de MAREVA
- les accusés réception du prestataire EDI

3.5.1.Accusés réception de MAREVA

En réponse à un message fonctionnel d'un prestataire EDI, le système MAREVA émet :

- un accusé de réception positif si aucune erreur n'a été détectée. **Le message EDI est sauvegardé puis transmis au téléservice concerné** ;
- un accusé de réception négatif si une erreur a été détectée soit dans le contenu du message soit lors de son traitement. **Le message EDI est ignoré.**

A noter que, conformément aux spécifications MAREVA (§ 4.3), l'accusé réception est contenu dans une pièce jointe document1.xml.

Les accusés de réception de MAREVA sont envoyés à l'adresse de messagerie FROM du message reçu du prestataire.

3.5.1.1.Exemple d'accusé de réception positif

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
```

```
<ReponseMAREVA>
```

```
<EnveloppeConnexion>
```

```
<connexionId>DGDDI</connexionId>
```

```
<interchangeAgreementId>test1</interchangeAgreementId>
```

```
<numEnveloppe>1</numEnveloppe>
```

```
<DateTime>
```

```
<date>19/05/05</date>
```

```
<time>11:49:38</time>
```

```
</DateTime>
```

```
<applicationId>diagnostic</applicationId>
```

```
</EnveloppeConnexion>
<Reponse>
  <numEnveloppe>1</numEnveloppe>
</Reponse>
</ReponseMAREVA>
```

Le deuxième numEnveloppe correspond au numEnveloppe du message du prestataire de connexion.
Le message applicatif réceptionné est sauvegardé et transmis au téléservice.

3.5.1.2.Exemple d'accusé de réception MAREVA négatif

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<ReponseMAREVA>
  <EnveloppeConnexion>
    <connexionId>DGDDI</connexionId>
    <interchangeAgreementId>UNKNOWN</interchangeAgreementId>
    <numEnveloppe>1</numEnveloppe>
    <DateTime>
      <date>19/05/05</date>
      <time>11:49:36</time>
    </DateTime>
    <applicationId>UNKNOWN</applicationId>
  </EnveloppeConnexion>
<ReponseErreur>
  <erreurCode>1</erreurCode>
  <erreurDescription>Le format XML de l'enveloppe n'est pas respecte.</erreurDescription>
  <numEnveloppe>1</numEnveloppe>
</ReponseErreur>
</ReponseMAREVA>
```

Ce message est rempli « au mieux » en fonction du degré de gravité de l'erreur: ici, par exemple, l'applicationId est inconnu.

Les champs de ReponseErreur sont:

- erreurCode: le code de l'erreur;
- erreurDescription: un libellé décrivant l'erreur;
- numEnveloppe: le numéro de l'enveloppe du message envoyé par l'opérateur.

Le message source n'est pas sauvegardé.

3.5.2.Accusés réception du prestataire EDI

Quand un message est émis vers un prestataire EDI, ce dernier doit transmettre un accusé réception de ce message, **indépendamment de la validité du contenu fonctionnel de ce message.**

Si l'accusé de réception n'est pas reçu, Mareva ré-émet le message deux fois jusqu'à bloquer les échanges avec le prestataire EDI au bout d'un délai paramétré.

3.5.2.1.Exemple d'accusé réception d'un prestataire de connexion

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<ReponseMAREVA>
  <EnveloppeConnexion>
    <connexionId>SIRET-PRESTATAIRE</connexionId>
    <interchangeAgreementId>test1</interchangeAgreementId>
    <numEnveloppe>1</numEnveloppe>
    <DateTime>
      <date>19/05/05</date>
      <time>11:49:38</time>
    </DateTime>
    <applicationId>diagnostic</applicationId>
  </EnveloppeConnexion>
</ARMareva>
  <numEnveloppe>1</numEnveloppe>
</ARMareva>
</ReponseMAREVA>
```

Le deuxième numEnveloppe correspond au numéro de l'enveloppe du message envoyé par la Douane.

3.6.CONSTITUTION D'UN MESSAGE EDI

Un message EDI est constitué d'une enveloppe de technique et d'une enveloppe fonctionnelle. Chaque enveloppe est unique par message.

L'enveloppe de connexion ou enveloppe technique est caractérisée par un numéro d'enveloppe **<numEnveloppe>**.

La dénomination de la balise identifiant l'enveloppe message varie en fonction du type de message.

Le contenu fonctionnel Douane d'un message est délimitée par une balise **</Message>**. Cette balise est unique dans un message fonctionnel.

3.6.1.Numéro d'enveloppe

C'est un numéro géré par l'expéditeur d'un message EDI : le prestataire EDI ou la Douane (MAREVA). Chacun gère sa propre série. Il y a un numéro d'enveloppe par message EDI.

Son identifiant dans l'enveloppe de connexion est l'élément **<numEnveloppe>**.

3.6.2.Identifiant de transaction

C'est un numéro unique obligatoire, géré par l'opérateur, qui permet de repérer sous une même référence tous les messages fonctionnels qu'il envoie ou reçoit et qui conduisent à des changements d'état d'un même objet depuis son état initial (création) jusqu'à son état final.

Ainsi l'identifiant de transaction du message fonctionnel de création d'une déclaration anticipée sera le même que celui du message fonctionnel de validation de cette même déclaration.

Il a été décidé que les applications douanières ne génèrent pas d'identifiant de transaction ni de numéro de séquence. Lorsqu'une application douanière envoie un message fonctionnel à un opérateur, elle fait référence au numéro de transaction de l'opérateur.

3.6.3. Numéro de séquence

C'est l'ordre d'un message fonctionnel dans une transaction. Il permet à MAREVA de délivrer les messages fonctionnels dans le bon ordre à l'application (il ne faut pas que le message fonctionnel de validation soit délivré avant le message fonctionnel de création). Il est attribué par l'opérateur. La Douane n'en fournit pas dans l'enveloppe de ses messages fonctionnels émis vers les opérateurs.



Le premier message d'une transaction a obligatoirement **le numéro de séquence zéro**.

A noter que si par exemple, la Douane a reçu les messages de numéro de séquence 0, 1, 5, 6. Les messages 5 et 6 sont conservés en mémoire une trentaine de minutes. Si les messages 2, 3, 4 ne sont pas envoyés dans ce délai, alors les messages 5 et 6 sont rejetés et une erreur 51 est envoyée pour chacun de ces messages.

4.PROTOCOLE D'ÉCHANGES MAREVA

4.1.ADRESSES DE MESSAGERIE

4.1.1.Côté Douane

Chaque téléservice possède une boîte fonctionnelle dans l'environnement de production.

L'adresse de messagerie de production est du type: « [teleprocedure](mailto:teleprocedure@edi.douane.finances.gouv.fr) »@edi.douane.finances.gouv.fr.

L'adresse de messagerie de l'application Diagnostic est : [diagnostic](mailto:diagnostic@edi.douane.finances.gouv.fr)@edi.douane.finances.gouv.fr.

4.1.2.Côté prestataire de connexion

Le prestataire de connexion doit fournir à la Douane pour chacun des téléservices qu'il est autorisé à utiliser :

- une adresse pour l'environnement de certification
- une adresse pour l'environnement de production



Les deux adresses doivent être différentes pour les deux environnements et leur dénomination le plus explicite possible.

N.B.1 : Pour **l'application Diagnostic** permettant de valider le caractère opérationnel de la connexion entre le SI de la Douane et le SI du prestataire, seule une adresse pour l'environnement de certification est nécessaire.

N.B.2 : Lors de la mise en place de l'interconnexion entre le SI de la Douane et le SI du prestataire, un test d'envoi et de réception simple est possible avec une boîte test de la Douane, permettant ainsi de valider la connectivité SMTP: [smtp-test](mailto:smtp-test@edi.douane.finances.gouv.fr)@edi.douane.finances.gouv.fr

N.B.3 : En mode d'interconnexion de production PASTEUR, l'adresse IP du serveur SMTP du prestataire de connexion doit aussi être fournie.

4.2.SERVEURS SMTP

Le prestataire de connexion émet des messages vers la Douane et doit pouvoir réceptionner des messages en provenance de la Douane.

Il dispose donc de boîtes aux lettres sur un service de messagerie pouvant recevoir les envois SMTP de la Douane (typiquement, un serveur ou un hébergeur lui proposant ces boîtes).

En revanche, les messages en provenance du prestataire de connexion peuvent être envoyés par différents moyens vers le serveur SMTP Douane edi.douane.finances.gouv.fr. Les modalités d'envoi dépendent du mode d'interconnexion et ne sont pas décrits dans ce document.

4.3.CONSTITUTION DES MESSAGES

4.3.1.Pièces jointes

Le message doit être de type MIME MULTIPART.

Il doit contenir deux fichiers attachés de type MIME « application/octet-stream ».

Ces deux fichiers attachés doivent être nommés « document1.xml » et « signature1.sig ». Le premier fichier contient le message EDI lui-même (dont le format XML suit la spécification d'enveloppe de connexion pour partie, et d'enveloppe de message pour le reste du contenu) et le deuxième fichier la signature de ce premier fichier.



Le message au sens courriel constitué de l'ensemble **n'est pas signé**.



Les pièces jointes doivent être encodées en base 64 avant leur envoi afin de conserver intact leur contenu.

4.3.2.Certificats

Un ou deux certificats X509 (1024 bits) 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 (1024 bits) 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

Les certificats prestataire de connexion doivent être obtenus auprès des autorités de certification agréés par le ministère des finances :

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

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

Le certificat doit être normalisé RGS. Idéalement, le certificat doit être de type « certificat de cachet ». Peu de PSCE proposent ce type de certificat et c'est pourquoi les certificats de type « certificat de société » ou « certificats SSL » sont acceptés à titre dérogatoire. Le niveau de sécurité RGS** (RGS deux étoiles) est conseillé.

Ces certificats doivent être fournis à la Douane lors de la mise au point du contrat de connexion. Ils sont enregistrés dans la relation PEDI (ROSA) du prestataire de connexion.

Important : Les certificats fournis à la douane doivent toujours être en cours de validité. Avant que la date de fin de validité soit atteinte, le prestataire de connexion EDI doit impérativement fournir un nouveau certificat valide à la Douane.

4.3.2.2.1Format 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

4.3.2.2 Exigences complémentaires

Pour des raisons d'optimisation du service Mareva, les certificats doivent répondre aux exigences complémentaires suivantes :

- avoir une taille de clé de 1024bits ;
- être signés avec les chiffres RSA et Sha-1 ;
- permettre la signature avec le chiffrement RSA ;
- avoir une période de validité d'au maximum deux ans et un mois.

Pour vérifier ces exigences, utiliser le visualisateur de certificat de Windows. Les noms des attributs à consulter sont respectivement, dans l'ordre des exigences: *clé publique*, *clé publique*, *algorithme de signature*, *valide à partir de* et *valide jusqu'à*.

4.3.3. Constitution du fichier de signature

La signature doit être de type « SHA1 » pour l'algorithme de condensation et « RSA » pour l'algorithme de chiffrement.

4.3.3.1. Quel outil ?

Il n'y a pas de recommandation.

La signature réalisée doit être équivalente à la commande openssl suivante :

```
openssl dgst -sha1 -sign cle-prive-RSA.pem -out signature document
```

où cle-prive-RSA est la clé privée de signature
signature est le fichier signature généré
document est le document signé

4.3.3.2. Comment vérifier la signature ?

La vérification cryptographique d'une signature s'effectue à l'aide de la commande :

```
openssl dgst -sha1 -verify cle -signature signature document
```

où cle est la clé publique extraite du certificat du signataire
signature est la signature à vérifier
document est le document signé

La clé peut être extraite du certificat avec la commande suivante :

```
openssl x509 -pubkey -noout -in certificat > cle
```

où cle est la clé publique extraite du certificat du signataire
cer est le certificat dont on cherche à extraire la clé publique

4.4. BLOCAGE ET DÉBLOCAGE DU PRESTATAIRE

4.4.1. Principe

Quand le système MAREVA transmet un message applicatif d'un téléservice douanier à l'adresse d'un prestataire de connexion, celui-ci doit acquitter le message en répondant par un accusé de réception. Si le message n'est pas acquitté dans un délai de vingt (20) minutes actuellement, il est automatiquement réémis deux fois dans un délai d'une heure.

Passé ce délai, le prestataire de connexion sera bloqué par le système MAREVA. Le blocage se fait par téléprocédure. Un **message d'erreur « 40 »** est envoyé au prestataire de connexion l'informant du blocage des échanges.

L'envoi des messages vers le prestataire de connexion pour l'application concernée est suspendu.

Les messages sont rejetés avec un **message d'erreur « 42 »** rappelant le blocage des échanges.

Pour se débloquer, le prestataire envoie une demande de déblocage auprès de Mareva. Le prestataire est débloqué pendant 20 minutes ce qui lui permet d'envoyer l'ensemble des messages en attente d'accusé réception. Si les messages en attente d'accusé réception ne sont acquittés auprès de Mareva, le prestataire sera de nouveau bloqué par Mareva entraînant l'envoi d'un message de blocage (message d'erreur 40).

4.4.2.Format des messages

4.4.2.1.Message de blocage

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<ReponseMAREVA>
  <EnveloppeConnexion>
    <connexionId>DGDDI</connexionId>
    <interchangeAgreementId>000541534</interchangeAgreementId>
    <numEnveloppe>3</numEnveloppe>
    <DateTime>
      <date>19/05/05</date>
      <time>11:49:36</time>
    </DateTime>
    <applicationId>Diagnostic</applicationId>
  </EnveloppeConnexion>
<ReponseErreur>
  <erreurCode>40</erreurCode>
  <erreurDescription>blocage après 3 tentatives de communication sans réponse.</erreurDescription>
  <numEnveloppe>0</numEnveloppe>
</ReponseErreur>
</ReponseMAREVA>
```

4.4.2.2.Déblocage

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<DemandeDeblocage>
<EnveloppeConnexion>
<connexionId>SIRET-PRESTATAIRE</connexionId>
<interchangeAgreementId>00000001</interchangeAgreementId>
<numEnveloppe>1</numEnveloppe>
<DateTime>
<date>01/01/05</date>
<time>00:00:00</time>
</DateTime>
<applicationId>nom application</applicationId>
</EnveloppeConnexion>
</DemandeDeblocage>
```

4.5. CONTRÔLES DES MESSAGES ENVOYÉS

4.5.1. Unicité des messages

Deux vérifications sont faites lors de la réception des messages par le système MAREVA :

1. unicité des messages techniques

Vérification d'unicité du triplet (**application, ConnexionId, numEnveloppe**) de l'enveloppe de connexion.

2. unicité des messages fonctionnels

Vérification d'unicité du quadruplet (**application, partyId, transactionId, numsequence**).

A la réception d'un doublon, le système MAREVA renvoie un message d'erreur et le message est ignoré.

4.5.2. Champs from et to du message

Les champs from et to d'un message doivent être correctement renseignés. S'ils ne le sont pas, le message sera complètement ignoré sans aucun accusé de réception.

4.5.3. Horodatage

Attention : le serveur MAREVA est synchronisé sur un serveur de temps PARIS, France Métropolitaine.

Les messages XML ont tous dans leur enveloppe leur date d'émission. Les documents XML étant arrivés **plus d'une demi-heure** après cette date seront systématiquement rejetés.

5. PROTOCOLE DE TEST

Est décrit ici le protocole de test d'un système devant communiquer avec le système MAREVA, ce qui ne préjuge pas du fonctionnement avec un téléservice douanier qui devra faire l'objet d'un protocole de tests applicatifs spécifique.

5.1. APPLICATION DE TEST

Une application de test simulant la réponse d'un téléservice est disponible et appelée **diagnostic**. Elle reçoit des messages du système du prestataire de connexion et renvoie des accusés de réception de test.

Son adresse de messagerie est : diagnostic@edi.douane.finances.gouv.fr

5.2. TESTS

Une dizaine de messages devront être envoyés par le système du prestataire de connexion; s'ensuivra l'envoi de 10 accusés de réception du système MAREVA et 10 messages de l'application diagnostic. Il est vérifié que les accusés de réception de l'opérateur ont bien été envoyés et reçus par le système MAREVA dans les délais impartis.

Les messages envoyés par le système du prestataire de connexion devront contenir une enveloppe de connexion et de message valides. Le contenu fonctionnel éventuel du message est ignoré.

5.3.VÉRIFICATIONS

Elles portent sur les conditions de production, ainsi:

- les signatures des messages sont vérifiées;
- l'intégration correcte des données du prestataire de connexion dans ROSA est vérifiée;
- le format des enveloppes est vérifié;
- l'unicité des messages est vérifiée;
- la séquence des messages est vérifiée;
- les délais sont vérifiés;
- les erreurs éventuelles sont signalées au système du prestataire de connexion.

5.4.CONDITIONS DE VALIDATION

Les dix messages envoyés par le système du prestataire de connexion auront du être acquittés par le système MAREVA. Les dix messages envoyés par l'application diagnostic en réponse devront avoir été acquittés correctement par le système de l'opérateur.

6.CORRESPONDANT MAREVA

Bureau C2, architecture technique et de sécurité

Téléphone secrétariat : 01.57.53.45.49

Mèl : connexion-edi@douane.finances.gouv.fr

7. TABLEAU DES ERREURS

Ce tableau rassemble toutes les erreurs susceptibles d'être renvoyées dans les accusés de réception négatifs.

Tous les messages d'erreur n'ayant pas la forme ci-dessous ne sont pas des messages issus du système MAREVA. Ils ont le plus souvent pour origine le téléservice auquel le message applicatif est destiné. Il convient alors de se reporter à la liste d'erreur du téléservice et le cas échéant de contacter le SAU Douane (cid-sau@douane.finances.gouv.fr) pour un complément d'information.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
```

```
<ReponseMAREVA>
```

```
  <EnveloppeConnexion>
```

```
    <connexionId>DGDDI</connexionId>
```

```
    <interchangeAgreementId>UNKNOWN</interchangeAgreementId>
```

```
    <numEnveloppe>1</numEnveloppe>
```

```
    <DateTime>
```

```
      <date>19/05/05</date>
```

```
      <time>11:49:36</time>
```

```
    </DateTime>
```

```
    <applicationId>UNKNOWN</applicationId>
```

```
  </EnveloppeConnexion>
```

```
<ReponseErreur>
```

```
  <erreurCode>1</erreurCode>
```

```
  <erreurDescription>Le format XML de l'enveloppe n'est pas respecte.</erreurDescription>
```

```
  <numEnveloppe>1</numEnveloppe>
```

```
</ReponseErreur>
```

```
</ReponseMAREVA>
```

Principe de fonctionnement en cas d'erreur MAREVA (accusé de réception négatif) :

Quand une erreur est détectée par le système, le message reçu est rejeté, les pièces jointes ne sont pas mémorisées. Aucune référence à ce message n'est enregistré.

Aussi n'est-il pas possible de vérifier le contenu du message par la Douane. Pour obtenir une aide, il convient de transmettre les pièces jointes document1.xml et signature1.sig ainsi que l'erreur retournée :

- à l'adresse connexion-edi@douane.finances.gouv.fr lors de la phase diagnostic
- au SAU douane cid-sau@douane.finances.gouv.fr lors de la phase production

N°	<i>Libellé</i>	<i>Explication</i>	<i>Action du prestataire de connexion/opérateur</i>
1	Le format XML de l'enveloppe n'est pas respecté	Le document envoyé en pièce jointe n'est pas au format XML spécifié par le protocole MAREVA.	Vérifier la structure XML du fichier document1.xml au regard des spécifications du protocole MAREVA. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
2	numseq manquant	Le champ <numseq> n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
3	numseq format invalide	Le champ numseq contient un caractère qui n'est pas un chiffre ou il dépasse 5 caractères de longueur.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
4	Date manquante	Le champ <date> n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
5	Time manquant	Le champ <time> n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
6	DateTime format invalide	Les champs date et time concaténés ne sont pas du type: dd/MM/yyHH:mm:ss	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
7	partyId manquant ou invalide	Le champ partyId n'est pas renseigné ou il contient des caractères non ASCII (seuls les codes ASCII des caractères de 32 à 127 sont acceptés).	Renseigner correctement le champ indiqué. Il s'agit du numéro d'agrément Douane de l'opérateur. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
8	interchangeAgreementId manquant ou invalide	Le champ interchangeAgreementId n'est pas renseigné ou il contient des caractères non ASCII (seuls les codes ASCII des caractères de 32 à 127 sont acceptés).	Renseigner correctement le champ indiqué. Il s'agit du numéro d'agrément Douane (PEDI) du prestataire de connexion. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
9	connexionId manquant ou invalide	Le champ connexionId n'est pas renseigné ou il contient des caractères non ASCII (seuls les codes ASCII des caractères de 32 à 127 sont acceptés).	Renseigner correctement le champ indiqué. Il s'agit du numéro d'agrément Douane (PEDI) du prestataire de connexion. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
10	applicationId manquant ou invalide	Le champ applicationId n'est pas renseigné ou il contient des caractères non ASCII (seuls les codes ASCII des caractères de 32 à 127 sont acceptés).	Renseigner correctement le champ indiqué. Il s'agit du numéro d'agrément Douane (PEDI) du prestataire de connexion. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
11	Le message n'est pas de type MIME	Le message envoyé à MAREVA doit être de type MIME.	Respecter le protocole exigé par le système MAREVA.
12	Le contenu du message n'est pas de type MIME multipart	Le message envoyé à MAREVA doit être de type MIME avec des attachements.	Le fichier document1.xml et sa signature signature1.sig doivent être en pièces attachées du message transmis à la douane (Content-Disposition: attachment)
13	Pièce jointe XML manquante	Le message doit contenir une pièce jointe nommée document1.xml qui contient le message XML EDI.	Vérifier le message envoyé et ajouter la pièce jointe manquante.
14	Message corrompu	Impossible de récupérer le contenu du message	Générer de nouveau le message avec les pièces jointes, éventuellement régénérées elles aussi. Il semble inutile de tenter de renvoyer le même message.
15	Enveloppe manquante	Le message ne contient pas les balises de l'enveloppe.	Vérifier le contenu du fichier document1.xml. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de numéro de séquence, s'ils étaient présents. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
16	Doublon d'enveloppe	Un message ayant le même numéro d'enveloppe a déjà été reçu et enregistré par le système MAREVA. L'identifiant d'unicité est le triplet (application, connexionId, numenveloppe).	Renvoyer le message en modifiant le numéro d'enveloppe, mais sans modification des numéros de transaction et de séquence. Modifier la date et heure d'envoi de la balise <DateTime>.
17	Trop de messages à séquencer	Erreur interne.	Le nombre de messages reçus pour une même transaction ne peut être traité par le système MAREVA. Il peut être nécessaire d'attribuer un nouveau numéro de transaction pour finaliser la transaction.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
18	numEnveloppe manquant	Le champ numEnveloppe n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
19	NumEnveloppe format invalide	Le champ numEnveloppe dépasse 10 caractères ou n'est pas composé uniquement de chiffres.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
20	Document1.xml contient un nombre de messages fonctionnels différent de 1	Un seul message fonctionnel est autorisé pour un même message technique.	Supprimer les messages fonctionnels pour qu'il n'en reste qu'un. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>. Créer autant de message que de messages fonctionnels à transmettre et procéder à leur envoi unitaire.
21	SchemaId manquant	Le champ schemaId n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
22	SchemaVersion manquant	Le champ schemaVersion n'est pas renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
23	TransactionId manquant ou invalide	Le champ transactionId n'est pas renseigné ou il contient des caractères non ASCII (seuls les codes ASCII des caractères de 32 à 127 sont acceptés).	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
24	Document1.xml mal encodé	Le document XML est mal encodé; un caractère est invalide.	<p>Le système MAREVA ne peut lire le fichier document1.xml.</p> <p>Le fichier document1.xml doit être encodé en "ISO-8859-1" ou un caractère est illisible.</p> <p>Vérifier à l'aide d'un parseur XML la validité du contenu du fichier document1.xml.</p> <p>Quand le contenu est valide, renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p>
25	applicationId format invalide	Ce champ contient plus de 15 caractères.	<p>Renseigner correctement le champ indiqué.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p>
26	InterchangeAgreementId format invalide	Ce champ contient plus de 20 caractères.	<p>Renseigner correctement le champ indiqué.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p>
27	NumEnveloppe format invalide	Ce champ dépasse en valeur les dix milliards.	<p>Renseigner correctement le champ indiqué.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p>
28	partyId format invalide	Ce champ dépasse 100 caractères.	<p>Renseigner correctement le champ indiqué.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p>

N°	<i>Libellé</i>	<i>Explication</i>	<i>Action du prestataire de connexion/opérateur</i>
29	idTransaction format invalide	Ce champ dépasse 15 caractères.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
30	numseq format invalide	Ce champ dépasse en valeur 1000.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
31	connexionId format invalide	Ce champ dépasse 20 caractères.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
32	ApplicationId incohérente	Le nom de l'application donné par le message Xml est différent de celui affecté à la boîte de messagerie.	Exemple : Dans document1.xml <applicationId>Diagnostic</applicationId>, le message est envoyé à deltad@edi.douane.finances.gouv.fr Vérifier le nom de l'application ou l'adresse de messagerie d'envoi et corriger celui qui est erroné. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
33	Deuxième numEnveloppe manquant	L'accusé de réception renvoyé par le prestataire de connexion a le deuxième champ numEnveloppe non renseigné.	Renseigner le champ manquant. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.

N°	<i>Libellé</i>	<i>Explication</i>	<i>Action du prestataire de connexion/opérateur</i>
34	Deuxième numEnveloppe invalide	Ce champ dépasse les dix chiffres ou contient un caractère autre qu'un chiffre.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
35	Deuxième numEnveloppe invalide	Ce champ dépasse les dix milliards.	Renseigner correctement le champ indiqué. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
36	InterchangeAgreementId inconnu	L'identifiant n'est pas répertorié dans le référentiel ROSA.	Le numéro d'agrément indiqué n'est pas connu du référentiel ROSA. Vérifier le numéro indiqué dans la balise <interchangeAgreementId>. Il doit être identique à celui fourni dans votre contrat de connexion. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
37	signature1.sig manquant	Le message envoyé à MAREVA ne contient pas la pièce jointe signature1.sig, c'est-à-dire la signature du message.	Construire le fichier de signature du fichier document1.xml et l'attacher en pièce jointe au message à destination du téléservice. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
38	signature invalide	La signature contenue dans le message ne correspond pas à la signature du fichier document1.xml à l'aide de l'un des certificats fournis par le prestataire de connexion.	<p>Vérifier le certificat de signature utilisé.</p> <p>Il est à noter que cette erreur survient, dans la majorité des cas, lorsque la pièce jointe document1.xml n'a pas été encodée en base 64 avant envoi. Dans ce cas, lors de l'intégration de la pièce jointe dans le message, des caractères de fin de ligne sont ajoutés qui modifient le fichier. Lors du contrôle réalisé par le système MAREVA consistant à appliquer le certificat contenu dans le référentiel ROSA à la pièce jointe document1.xml, le fichier de signature n'est pas identique au fichier signature1.xml transmis lors de l'envoi du message.</p> <p>Procéder à l'encodage de la pièce jointe sans modification des numéros d'enveloppe, de transaction et de séquence. Par contre modifier la date et heure d'envoi de la balise <DateTime>.</p> <p>Renvoyer le message.</p>
39	Certificat invalide	Aucun des certificats présents dans le référentiel ROSA ne sont des certificats valides.	<p>Vérifier auprès du service certification du CID (certification-edi@douane.finances.gouv.fr) les certificats contenus dans le référentiel ROSA.</p>
40	Blocage des échanges	Un message a été réémis trois fois, dans un délai d'une heure, sans réponse de la part du prestataire (accusé de réception). Le système MAREVA bloque alors les échanges avec le prestataire de connexion pour l'application concernée.	<p>L'envoi des messages à destination de ce prestataire de connexion est suspendu.</p> <p>Suspendre l'envoi de messages applicatifs, envoyer une demande de déblocage puis les accusés de réception attendus par le système.</p>
41	Délai dépassé	Le message a un DateTime d'émission inférieur à la date de réception de plus de 30 minutes.	<p>Le système MAREVA rejette tous les messages dont la date d'envoi est supérieur de 30 minutes à la date de réception.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.</p>

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
42	Echange bloqué – attente d'AR	Le système MAREVA a bloqué les échanges avec le prestataire de connexion et rejette tous les messages de l'application concernée jusqu'au déblocage.	Suspendre l'envoi de messages applicatifs et envoyé une demande de déblocage puis les accusés de réception attendus par le système.
43	Numéro d'enveloppe douane invalide	Le numéro d'enveloppe présent dans l'accusé de réception de l'opérateur n'est pas connu du système MAREVA.	Le système MAREVA ne connaît pas le numéro d'enveloppe indiqué (dans le contexte du téléservice référencé <applicationId>. Vérifier le numéro d'enveloppe indiqué dans l'accusé de réception. Renvoyer le message sans modification du premier numéro d'enveloppe. Par contre modifier la date et heure d'envoi de la balise <DateTime>.
44	Relation PEDI désactivée	Dysfonctionnement du référentiel ROSA	Une intervention Douane est nécessaire. A la résolution du problème, renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.
45	Relation PEDI corrompue	Dysfonctionnement du référentiel ROSA	Une intervention Douane est nécessaire. A la résolution du problème, renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.
46	ConnexionId autre que celui indiqué par InterchangeAgreementId	Le champ connexionId de l'enveloppe du message ne correspond pas à celui indiqué par la relation PEDI du référentiel ROSA.	Vérifier le contenu des deux balises. Le cas échéant, prendre contact avec le service de certification du CID (certification-edi@douane.finances.gouv.fr), pour vérifier les informations du référentiel ROSA. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.

N°	<i>Libellé</i>	<i>Explication</i>	<i>Action du prestataire de connexion/opérateur</i>
47	InterchangeAgreementId de l'AR différent de celui en base	L'accusé de réception du prestataire de connexion référence un message douanier dont l'InterchangeAgreementId ne correspond pas au prestataire de connexion expéditeur.	Vérifier le contenu du champ. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.
48	Pièce jointe document1.xml corrompue	Le message reçu par MAREVA contient une pièce jointe document1.xml illisible.	Modifier les pièces jointes du message. Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.
49	Erreur lors de l'écriture du message	Le message n'a pu être sauvegardé par le système MAREVA.	Une intervention Douane est nécessaire. A la résolution du problème, renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.
50	Accès au référentiel ROSA impossible	Le référentiel ROSA est inaccessible.	Une intervention Douane est nécessaire. A la résolution du problème, renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.

N°	Libellé	Explication	Action du prestataire de connexion/opérateur
51	Message hors séquence consécutive expiré	Le numéro de séquence de ce message n'est pas immédiatement supérieur au dernier reçu pour la même transaction; le délai d'attente imparti de 30 minutes est dépassé.	<p>Le système MAREVA assure la séquence des messages dans une transaction. A chaque réception, il compare le numéro de séquence du message avec le dernier reçu. Si aucun message n'a été reçu pour la transaction, le premier numéro de séquence doit être zéro.</p> <p>Si le numéro n'est ni zéro ni le dernier numéro de séquence + 1, le message est conservé en attente. Au bout de 30 minutes, il est rejeté, sa durée de validité étant atteinte.</p> <p>Le numéro de séquence attendu est indiqué dans le message erreur 51 retourné.</p> <p>Vérifier le numéro de séquence.</p> <p>Renvoyer le message sans modification du numéro d'enveloppe. Il peut être nécessaire de modifier soit le numéro de séquence soit de transaction. Dans tous les cas, modifier la date et heure d'envoi de la balise <DateTime>.</p>
52	Pièce jointe signature1.sig corrompue	Le message reçu par MAREVA contient une pièce jointe signature1.sig illisible.	<p>Reconstruire le fichier de signature du fichier document1.xml.</p> <p>Modifier les pièces jointes du message.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.</p>
53	Plus d'une pièce jointe document1.xml	Le message reçu par MAREVA contient plus d'une pièce jointe document1.xml	<p>Reconstruire le message en y intégrant un fichier unique document1.xml et le fichier de signature correspondant.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.</p>

<i>N°</i>	<i>Libellé</i>	<i>Explication</i>	<i>Action du prestataire de connexion/opérateur</i>
54	Plus d'une pièce jointe signature1.sig	Le message reçu par MAREVA contient plus d'une pièce jointe signature1.sig	<p>Reconstruire le message en y intégrant un fichier unique document1.xml et le fichier de signature correspondant.</p> <p>Renvoyer le message sans modification des numéros d'enveloppe, de transaction et de séquence. Mais modifier la date et heure d'envoi de la balise <DateTime>.</p>
55	Doublon de message fonctionnel	Un message ayant le même numéro de transaction et de séquence a déjà été reçu et enregistré par l'application MAREVA. L'identifiant d'unicité est le quadruplet (applicationId, partyId, transactionId, numseq).	<p>Vérifier les différents champs d'identifiant d'unicité.</p> <p>Modifier le ou les champs incriminés (partyId ou transactionId ou numseq).</p> <p>Renvoyer le message avec la nouvelle valeur changée pour le champ incriminé.</p>

Le tableau ci-dessus présente la marche à suivre en cas de réception d'un message d'erreur de la part du système MAREVA.

Il peut également survenir une interruption des échanges : le prestataire de connexion ne reçoit qu'un certain type de message (que les messages techniques ou que les messages applicatifs) ou encore il ne reçoit pas dans le délai court « habituel » l'accusé réception du système MAREVA.

Pour ce dernier cas, il faut envisager que le message transmis **ne respecte pas la séquence attendue** pour la transaction concernée. Aussi l'accusé de réception, qui sera négatif, **ne parviendra pas avant un délai de 30 minutes, durée de validité du message.**

Avant toute saisie du SAU douane, il convient de faire un pré-diagnostic, présenté dans **la fiche d'aide à la qualification d'anomalies EDI** disponible sur pro.douane.gouv.fr.

ANNEXE A : ELEMENTS POUR LA SIGNATURE ELECTRONIQUE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 847 (0x34f)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=FR, O=DIRECTION GENERALE DES DOUANES ET DROITS INDIRECTS, OU=0002 120023015, CN=DGDDI AC Signature

Validity

Not Before: Jun 6 12:04:49 2007 GMT

Not After : Jun 6 12:04:49 2009 GMT

Subject: C=FR, O=DIRECTION GENERALE DES DOUANES ET DROITS INDIRECTS, OU=0002 120023015,

OU=PERSONNES/serialNumber=58005/x500UniqueIdentifier=xdelannoy-dgddi, CN=Xavier DELANNOY

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ca:1a:40:ee:4a:d9:46:15:3f:57:f5:3a:76:08:
63:9a:a6:cf:a8:f2:07:54:26:8a:65:f8:4d:32:a5:
db:56:2b:85:ca:f7:a2:33:fd:61:e8:c0:4d:64:03:
91:99:e1:bb:ad:25:ad:fd:4a:fa:f7:d5:b1:da:d7:
78:63:30:69:0f:da:12:0d:a9:de:73:d0:d6:12:9c:
66:bd:19:e4:5e:27:43:05:9d:58:1a:e6:d9:b4:cb:
8d:da:a1:ce:4f:6f:53:a9:f4:7b:9f:c6:86:dc:45:
83:f9:b8:c5:35:20:c5:b7:7a:59:9a:8e:ad:c2:40:
da:0c:de:53:91:8d:12:16:b1

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

22:4A:D3:FB:17:04:E9:E0:0E:83:9D:6C:5B:EC:C9:D4:65:E8:4E:81

X509v3 Authority Key Identifier:

keyid:15:8D:DA:F3:BC:85:DD:23:83:48:CA:5D:C2:00:81:16:DC:0C:FB:76

X509v3 Certificate Policies:

Policy: 1.2.250.1.131.1.4.10.3.1.3

X509v3 Extended Key Usage:

E-mail Protection

X509v3 Key Usage: critical

Digital Signature, Non Repudiation

X509v3 Subject Alternative Name:

email:xavier.delannoy@douane.finances.gouv.fr

X509v3 CRL Distribution Points:

URI:http://crl.douane.gouv.fr/CADO_SignAC.crl

Authority Information Access:

OCSP - URI:http://ocsp.douane.gouv.fr/ocsp

Signature Algorithm: sha1WithRSAEncryption

83:02:8d:df:8e:f3:08:3a:bb:28:f8:14:f6:9f:03:29:88:ed:
a0:36:c5:3e:e6:43:df:31:9f:d9:83:fb:06:97:cf:bc:5a:1c:
e6:1d:1d:5a:a0:76:15:5b:0f:e5:f4:7d:e0:9f:e3:32:4c:99:
fd:76:96:f4:4d:f8:5a:dd:3d:e1:20:01:2b:27:ea:e6:e3:ce:
76:35:81:84:49:3e:6e:f3:b5:db:a1:ae:b7:8a:18:77:8c:f9:
44:fe:77:e5:12:bb:dd:83:05:55:ad:15:b7:c3:3d:c5:ea:15:
67:29:a7:20:4d:51:77:09:4f:b1:7e:35:1d:14:11:66:a3:2b:
40:4c:d3:f4:94:98:bd:d1:56:ad:db:f3:9a:10:b5:ed:b4:7f:
7e:b5:8f:80:88:ef:6f:7c:3a:fa:a6:26:2b:d6:3a:e5:3b:5a:
4c:6e:cc:c0:aa:c9:a2:98:3e:13:99:62:58:23:9a:d3:5a:c6:
02:63:3f:8b:1f:de:39:5e:86:84:65:82:5c:b0:35:71:26:db:
03:e2:3a:f6:81:5a:dd:d7:0c:a0:20:81:ab:e9:71:d1:2d:c2:
e5:de:87:e3:d0:b1:eb:a8:eb:3a:d1:48:2e:68:00:a0:f8:dd:
49:a7:7d:7c:58:c1:53:1e:4e:ad:08:6c:3a:5a:d3:48:d9:44:
a7:6e:06:af