DGDDI/DGC2/PP	**Foire Aux Questions : Mareva pour les opérateurs**	Référence	FAQ_Mareva_Operateurs_0.8.4
		Version	0.8.4

Table des matières

1 Spécifications de Mareva

1.1 La signature électronique et l'encodage des pièces-jointes

Cette fonctionnalité de Mareva est souvent la plus ardue à mettre en place pour l'établissement d'une connexion avec le guichet EDI.

1.1.1 La signature est invalide alors que le certificat est enregistré dans ROSA et j'utilise bien celui-ci ?

C'est fort probablement un problème d'encodage: les messages XML (texte) passés en pièces-jointes dans la messagerie sont transformés par les relais de messagerie (changements sur les fins de ligne). Donc la signature qui est celle du fichier original n'est plus conforme. C'est aussi vrai pour des envois manuels. Pour des tests manuels, demandez un format binaire (dans un zip par exemple). Pour les programmes, il faut FORCER l'encodage du fichier XML en base64. Le système attend un fichier binaire signature1.sig (signature du document1.xml en pièce-jointe, codée en base 64).

Le message électronique doit être encodé en multipart/mixed et doit contenir un corps de type de contenu text/plain et 2 pièces jointes 'document1.xml' et 'signature1.sig' (disposition `attachment` et non `inline`) de type de contenu application/octet-stream encodées au format base64.

Voici un exemple de message avec les bonnes informations (semblable à un message que Mareva envoie pour chaque réponse) :

```
Return-Path: <c2test1@edisimulation.douane.finances.gouv.fr>
Received: from murder ([unix socket]) by
         edisimulation.douane.finances.gouv.fr (Cyrus v2.2.12-Invoca-
         RPM-2.2.12-3.RHEL4.1) with LMTPA; Tue, 02 Feb 2010 13:40:05
          +0100
Received: from P401070 (unknown [10.141.31.177]) by CADOCRLDouane1
          (Postfix) with ESMTP id 37F12F24E92;
          Tue,  2 Feb 2010 13:40:05 +0100 (CET)
Subject: Enveloppe 111 - Transaction tid000111
From: "Diagnostic2 DGDDI/C2"
<c2test1@edisimulation.douane.finances.gouv.fr>
To: <diagnostic2@edi.douane.finances.gouv.fr>
Cc: <c2test1@edisimulation.douane.finances.gouv.fr>
Date: Tue, 02 Feb 2010 13:39:48 +0100
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="=-h5MDrmle4q7bb0s"
Message-Id: <20100202124005.37F12F24E92@CADOCRLDouane1>

--=-h5MDrmle4q7bb0s
Content-Type: text/plain

C2TEST BODY


--=-h5MDrmle4q7bb0s

Content-Transfer-Encoding: base64
Content-Type: application/octet-stream; name="signature1.sig"
Content-Disposition: attachment; filename="signature1.sig"

eN3nQ3kpjy78A7xaDjvpgKCosZ+FibFtlbmC1KyJ7XVsFvSB0qUs5RCFN54QWSd2xDLzM1n5
YhwxjEBtvFFo3uNA/VfDO1lHsNL/0lDXoECTpxji7XKKVFkWimZcokyPncKhPDyGXJj8t1tP
XH4/9eogrFxygaB+FrvKZLBqGJc=
```

```
--=-h5MDrmle4q7bb0s

Content-Transfer-Encoding: base64
Content-Type: application/octet-stream; name="document1.xml"
Content-Disposition: attachment; filename="document1.xml"
```


```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iSVNPLTg4NTktMSIgc3RhbmRhbG9uZT0i
eWVzIiA/Pgo8TWVzc2FnZU9wZXJhdGV1ciB4bWxuczp4c2k9Imh0dHA6Ly93d3cudzMub3Jn
LzIwMDEvWE1MU2NoZW1hLWluc3RhbmNlIiB4c2k6bm9OYW1lc3BhY2VTY2hlbWFMb2NhdGlv
bj0iTWVzc2FnZURlY0ltcC54c2QiPgogIDxFbnZlbG9wcGVDb25uZXhpb24+CiAgICA8Y29u
bmV4aW9uSWQ+MTIwMDIzMDE1PC9jb25uZXhpb25JZD4KICAgIDxpbnRlcmNoYW5nZUFncmVl
bWVudElkPjAwMDAwMDEyPC9pbnRlcmNoYW5nZUFncmVlbWVudElkPgogICAgPG51bUVudmVs
b3BwZT4xMTE8L251bUVudmVsb3BwZT4KICAgIDxEYXRlVGltZT4KICAgICAgPGRhdGU+MDIv
MDIvMTA8L2RhdGU+CiAgICAgIDx0aW1lPjEzOjM5OjQ3PC90aW1lPgogICAgPC9EYXRlVGlt
ZT4KICAgIDxhcHBsaWNhdGlvbklkPkRpYWdub3N0aWMyPC9hcHBsaWNhdGlvbklkPgogIDwv
RW52ZWxvcHBlQ29ubmV4aW9uPgogIDxNZXNzYWdlcz4KICAgIDxNZXNzYWdlPgogICAgICA8
RW52ZWxvcHBlTWVzc2FnZT4KCQkgPHNjaGVtYUlEPk1lc3NhZ2VEZWNJbXA8L3NjaGVtYUlE
PgoJCSA8c2NoZW1hVmVyc2lvbj4xLjE8L3NjaGVtYVZlcnNpb24+CgkJIDxwYXJ0eUlkPjEy
MDAyMzAxNTwvcGFydHlJZD4KCQkgPHRyYW5zYWN0aW9uSWQ+dGlkMDAwMTExPC90cmFuc2Fj
dGlvbklkPgoJCSA8bnVtc2VxPjA8L251bXNlcT4KICAgICAgPC9FbnZlbG9wcGVNZXNzYWdl
PgogICAgICA8RGVjbGFyYXRpb24+PC9EZWNsYXJhdGlvbj4KICAgIDwvTWVzc2FnZT4KICA8
L01lc3NhZ2VzPgo8L01lc3NhZ2VPcGVyYXRldXI+Cg==
```


```
--=-h5MDrmle4q7bb0s--
```

1.1.2 Comment générer le fichier signature à partir d'un fichier XML

Cette génération est laissée à l'appréciation du développeur du logiciel. Comme indiqué dans la spécification, la signature est de type RSA (PKCS#1) pour l'algorithme de chiffrement et SHA1 pour l'algorithme de condensation. Un fichier signature doit être généré pour chaque fichier XML différent à envoyer vers le guichet EDI.

Voici une méthode avec le logiciel libre `openssl` disponible sur de nombreuses plate-formes pour comparer la signature générée par votre logiciel avec celle qui sera acceptée par Mareva :

1. La clé **privée** de votre certificat opérateur doit être encodée au format PEM sans cryptage : le fichier doit être de la forme :

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBA
MIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBA
MIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBAMIICXAIBA
-----END RSA PRIVATE KEY-----
```

2. Générer la signature du fichier document1.xml avec la clé privée préalablement extraite

```
$ openssl dgst -sha1 -binary -sign cle-prive-RSA.pem -out \
signature1.sig document1.xml
```

3. La clé **publique** de votre certificat opérateur peut être extraite avec la commande suivante :

```
$ openssl x509 -pubkey -noout -in certificat.pem -out cle-
publique.pem
```

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

```
$ openssl dgst -sha1 -verify cle-publique.pem -signature
signature1.sig document1.xml
```

Le résultat doit être OK :

```
Verified : OK
```

1.1.3 Comment vérifier la signature des messages émis par la DGDDI

Voici une méthode avec le logiciel libre openssl disponible sur de nombreuses plate-formes pour comparer la signature générée par le logiciel avec celle qui sera acceptée par Mareva :

1. Récupérer le certificat de signature de la DGDDI sur le site https://pro.douane.gouv.fr et la sauvegarder dans un fichier certificat.pem, son contenu doit être le suivant :

```
-----BEGIN CERTIFICATE-----
MIIB+jCCAWOgAwIBAgIJAKIGJBGXqI8sMA0GCSqGSIb3DQEBBAUAMD8xDzANBgNV
BAMTBm1hcmV2YTEsMCoGCSqGSIb3DQEJARYdZGctYzJAZG91YW5lLmZpbmFuY2Vz
LmdvdXYuZnIwHhcNMDkwOTAxMDAwMDAyWhcNMTAxMjAxMDAwMDAyWjA/MQ8wDQYD
VQQDEwZtYXJldmExLDAqBgkqhkiG9w0BCQEWHWRnLWMyQGRvdWFuZS5maW5hbmNl
cy5nb3V2LmZyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/ySGkOtqQOaLG
1unj5shDnud0kN5KJxNm6bvdXfEr7Ihwz7bmML4eZK+AYcdeENmKCGmUiMZjpi5U
UvNMKSCA815DdeMQiCuwVFR7fYj6YqcuiPX3UrDjsbklL73yIvo0TxjZtGSG98ZR
drE+26+Q0wyYa4tEoZTu+cjL7bKV9wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHeh
T1j4fMDKs07iUYkbMWoLMkTM+eW0ONGg0Ejt6Ci++yE4tKm5Phz7bMVlq3Fu/Zcx
wI0vdbrDH0HNhP8NQxXYDGcDDquWTtI/E9IjPvxrrfoxXBn1meomyHH+ApTs2m5e
OCtHYLP7TEvyqpwyQqVtw4x0gTVjQ2FD1aWjg7eM
-----END CERTIFICATE-----
```

2. Extraire la clé publique du certificat :

```
$ openssl x509 -pubkey -noout -in certificat.pem -out cle-
publique.pem
```

3. Extraire les fichiers document1.xml et signature1.sig du message électronique émis par la DGDDI et les placer dans le même répertoire ;
4. Vérifier la signature par la commande suivante :

```
$ openssl dgst -sha1 -verify cle-publique.pem -signature \
signature1.sig document1.xml
```

Le résultat doit être OK :

```
Verified : OK
```

1.1.4 Format de signature : pourquoi Mareva n'utilise pas le standard PKCS#7 ?

Les raisons sont multiples :

- le système a été conçu en couches et a évolué durant sa conception,
- le choix de la messagerie SMTP pour l'échange des messages EDI est un choix de transport, d'autres options ont été envisagées (mais non confirmées), la seule capacité demandée est de pouvoir transmettre des PJ sans déformation du contenu,
- la signature n'est pas liée aux technologies de messagerie mais aux données transmises, et le mécanisme peut évoluer indépendamment de ce que fournissent les messageries,
- elle pourrait notamment évoluer sous forme de fichiers multiples ou conjoints, éliminant de fait la signature électronique d'un unique message,
- en terme d'usage, le format PKCS#7 est intéressant pour de la messagerie inter-personnelle, il n'apporte rien pour les flux EDI.

2 Fonctionnement de Mareva

2.1 Vérification des alertes

Avant toute chose, il vous faut vérifier sur le site Pro.douane : https://pro.douane.gouv.fr/prodouane.asp si aucune alerte n'est en cours pour les télé-procédures que vous utilisez en mode EDI. La description de l'alerte doit normalement contenir une liste des télé-procédures et éventuellement des prestataires EDI concernés. Si l'alerte concerne tous les opérateurs EDI, il faut attendre la levée de l'alerte ; le trafic devrait reprendre normalement dès ce moment-là.

2.2 Connectivité SMTP

2.2.1 Je n'arrive pas à envoyer de messages électroniques à Mareva

Pour vérifier où se situe le problème, il faut appliquer toutes les étapes de la fiche d'aide à la qualification d'anomalie EDI disponible sur Pro.douane : https://pro.douane.gouv.fr/download/downloadUrl.asp?file=PubliwebBO/fichiers/FicheConsignePrestatairesEDI-V2.pdf.

Si le déroulement de cette fiche ne suffit pas à diagnostiquer l'origine du problème, il faut ouvrir une demande d'assistance par TSAR sur Pro.douane : https://pro.douane.gouv.fr/tsar/TSAR_form.asp, il faudra **impérativement** joindre tous les résultats obtenus par le déroulement de la fiche.

2.2.2 Mes messages partent mais je reçois un message d'erreur

Ce message (dont le contenu va être similaire à cet extrait ci-dessous) est émis par votre serveur de messagerie vers l'adresse d'émission parce qu'il n'a pas réussi à transmettre le message électronique vers le serveur de messagerie de la DGDDI.

```
Reporting-MTA: dns; yourmailserveur
X-Postfix-Queue-ID: 2767FF2525D
X-Postfix-Sender: rfc822; yourmailadress@your.domain
Arrival-Date: Thu, 21 Jan 2010 14:32:02 +0100 (CET)
```

```
Final-Recipient: rfc822; application@edi.douane.finances.gouv.fr
Action: failed
Status: 5.0.0
Diagnostic-Code: X-Postfix; host 10.94.110.11[10.94.110.11] said: 554
    <application@edi.douane.finances.gouv.fr>: Recipient address rejected:
    Access denied (in reply to RCPT TO command)
```

Si le message d'erreur (partie en ***gras italique*** du message) contient '***Recipient address rejected***', la cause est que l'adresse d'émission n'est pas autorisée dans les filtres d'accès au serveur de messagerie. Il vous faut vérifier que votre adresse d'émission correspond bien à l'adresse indiquée sur le document « TODO : trouver le nom de la fiche certification » pour l'application visée.

- Si cette adresse d'émission n'est pas correcte de votre côté, il vous faut créer une boîte avec le nom correct et paramétrer votre logiciel d'échanges avec le guichet EDI pour qu'il utilise l'adresse connue par la DGDDI
- Si votre adresse d'émission est identique à celle indiquée dans la fiche, la configuration du filtre n'est pas correcte du côté du serveur de messagerie de la DGDDI. Il faut que vous ouvriez une demande d'assistance pour que cette adresse soit intégrée dans le filtre.

2.2.3 Mes messages partent mais je ne reçois pas d'accusés de réception Mareva

Tout d'abord, il faut vérifier qu'il n'y a bien qu'**un seul destinataire** (champ To: du message) pour les messages électroniques que vous émettez. Si plusieurs destinataires sont présents dans ce champ, Mareva ignore purement et simplement le message. Il est par contre possible de spécifier plusieurs destinataires qui recevront une copie carbone (champ Cc: du message).

Si ce n'est pas le cas, voici les tests à effectuer pour diagnostiquer le problème :

1. Il faut tout d'abord vérifier que les messages envoyés ne sont pas bloqués sur votre serveur de messagerie. Il doit posséder une interface qui permet de voir les messages dans la queue d'envoi. Si la connexion entre les 2 serveurs de messagerie est interrompue, les messages doivent être stockés par votre serveur de messagerie et il essaie de renvoyer tous les messages en erreur (retry) à des intervalles définis dans sa configuration. Dans ce cas, il faut vous reporter au cas décrit au 2.2.1 pour la résolution du problème.
2. Si les messages sont bien expédiés vers le serveur de messagerie de la DGDDI, il faut chercher dans les traces de votre serveur de messagerie l'heure du dernier message transmis par la DGDDI à votre intention. Si les traces indiquent que des messages sont transmis par la DGDDI, il faut regarder dans votre infrastructure si les messages ne se perdent pas lors de leur transmission dans les boites à lettres.
3. Sinon, selon le mode de connexion au guichet EDI :
   a) cas Pasteur : si plus aucun trafic ne transite sur le lien Pasteur dans le sens DGDDI => opérateur, il faut ouvrir un ticket d'incident auprès du support Pasteur en vous reportant à la fiche consigne fournie par le prestataire Pasteur.
   b) cas EDI - : il faut faire appel à l'éditeur de votre logiciel qui est tenu de vous aider dans le diagnostic de votre problème de connectivité.

2.2.4 Je n'arrive pas à expédier mes messages électroniques par le canal Pasteur léger/garanti

Il faut configurer correctement le serveur de messagerie qui expédie les messages à destination de la DGDDI. Pour se faire, il faut connaître l'adresse du serveur de messagerie du guichet EDI de la

DGDDI.

La configuration consiste à router tous les messages à destination du domaine `edi.douane.finances.gouv.fr` vers le serveur de messagerie précité. Cette configuration dépend du logiciel de serveur de messagerie que vous utilisez. Ce document ne couvre pas cette étape, les informations nécessaires se trouvent dans la documentation de votre serveur de messagerie.

2.2.5 Les messages émis par le Guichet EDI ne passent pas par le lien Pasteur léger/garanti mais arrivent par Internet

Cela indique que la configuration du serveur de messagerie du guichet EDI n'est pas correcte. Le routage du nom du domaine que vous utilisez pour vos échanges EDI avec la DGDDI n'utilise pas le lien Pasteur mais utilise la route par défaut qui transite par Internet. Ce domaine correspond à la partie postérieure au caractère '@' dans les adresses que vous utilisez (ici your.domain dans `yourmailadress@`***`your.domain`***).

Il faut ouvrir un ticket d'incident auprès du prestataire hébergeant le guichet EDI et indiquer dans votre demande le type d'incident : routage de messagerie Mareva et le domaine qui est en cause. Le prestataire retrouvera les informations de routage nécessaire et changera ce routage. Il prendra ensuite contact avec vous pour valider la correction.

2.3 Erreurs techniques Mareva

Lorsque le contenu du message électronique reçu n'est pas conforme aux attentes de Mareva, un message d'erreur est émis pour indiquer la source de l'erreur. Le message d'erreur est dans la quasi-totalité des cas émis juste après la réception du message par la DGDDI (hormis les erreurs de type 51 qui sont émises 30 minutes après la réception du message)

VOTRE LOGICIEL DOIT TRAITER TOUTES LES ERREURS MAREVA POUR ÊTRE CERTIFIÉ.

2.3.1 Erreur 11 : *Le message n'est pas de type MIME.*

Le champ 'Mime-Version: 1.0' doit être présent dans les entêtes du message électronique.

2.3.2 Erreur 12 : Le contenu du message n'est pas de type MIME multipart.

Le Content-type du message électronique doit être multipart/mixed.

2.4 Erreurs fonctionnelles Mareva

2.4.1 Erreur 51 : Message hors séquence consécutive expiré.

Ce message est reçu normalement une demi-heure après l'expédition du message d'enveloppe correspondant. Cette erreur est normalement due au contenu du champ `<numseq>` Par défaut, un message a une durée de validité de 30 minutes. Pour une transaction donnée, Mareva maintient un séquencement incrémental à travers ce champ. Si Mareva reçoit un message avec un numéro de séquence strictement supérieur à celui attendu (qui correspond au dernier numéro de séquence échangé incrémenté d'une unité), il met le message en attente de traitement pour attendre la réception le message qui contiendrait le ou les messages de cette même transaction avec le numéro de séquence attendu. Si ce message n'arrive pas dans un délai de 30 minutes, la durée de validité du

message initial expire et un message d'erreur 51 est envoyé.

3 Certification Mareva

3.1 Les étapes de la procédure de certification

3.1.1 Qui valide la phase diagnostic (phase MAREVA) ?

Ce sont les services de la Douane qui vous informent de la réussite de la phase MAREVA. Ils reprennent contact avec vous pour organiser la phase de certification de la télé-procédure que vous avez choisie.

4 Création de la PEDI dans ROSA :

4.1 Questions générales

4.1.1 Quels sont les informations nécessaires pour l'ouverture d'une connexion

Il faut **impérativement** fournir les informations suivantes dès l'envoi de la fiche de connexion pour préparer la configuration du système (filtrage de messagerie) et établir la relation PEDI dans ROSA :

- 1 adresse de messagerie pour les premiers tests de connexion au guichet EDI : utilisation de l'application Diagnostic,
- 1 adresse de messagerie par application de certification,
- 1 adresse de messagerie par application de production (si le titulaire de la PEDI a vocation à se connecter au guichet EDI en production),
- 1 certificat X.509 : pendant la période de certification, ce certificat peut être un certificat auto-signé ; toutefois, le certificat définitif conforme PRISv1 doit être obligatoirement fourni avant toute mise en production de l'opérateur EDI.

La fourniture d'une seule adresse de messagerie commune pour toutes les applications (diagnostic, certification et production) n'est pas autorisée. Pour le traitement des demandes d'assistance, il faut pouvoir distinguer facilement quelles adresses sont utilisées et isoler les émissions/réceptions.

4.2 Questions sur les adresses mails

4.2.1 Quels sont les formats d'adresses de messagerie autorisés ?

Le système de messagerie inter-applicative ne supporte qu'un sous-ensemble des adresses définies par la RFC 822 : les commentaires, caractères accentués, espaces ne sont pas autorisés.

4.3 Questions sur les certificats

4.3.1 Doit-on fournir un certificat de collaborateur (représentant légal) ou un certificat serveur (au nom de la société)

Dans le cas du prestataire EDI, il faut fournir un certificat serveur, dans le cas d'un opérateur EDI,

un certificat de collaborateur (nominatif) suffit.

4.3.2 Quelle est la classe de certificat minimale (parmi les classes 2, 3 et 3+) ?

Le certificat doit être de classe 2 au minimum.

4.3.3 Un prestataire EDI doit-il avoir un certificat par client ?

Non, un prestataire EDI n'utilise qu'une seule relation PEDI et il ne peut y être attaché qu'un seul certificat (avec un certificat secours au besoin).

4.3.4 Sous quelle forme doit-on transmettre les certificats

Les certificats de signature ou de chiffrement doivent être envoyés sous forme de fichier dont l'extension se termine par '`.crt`'. Le fichier doit être un fichier texte dont le contenu est votre certificat binaire DER encodé au format base 64.

Le fichier envoyé doit pouvoir s'ouvrir avec un éditeur de texte brut (par exemple un bloc note) et son contenu doit avoir cette forme :

```
-----BEGIN CERTIFICATE-----
MIIB+jCCAWOgAwIBAgIJAKIGJBGXqI8sMA0GCSqGSIb3DQEBBAUAMD8xDzANBgNV
BAMTBm1hcmV2YTEsMCoGCSqGSIb3DQEJARYdZGctYzJAZG91YW5lLmZpbmFuY2Vz
LmdvdXYuZnIwHhcNMDkwOTAxMDAwMDAyWhcNMTAxMjAxMDAwMDAyWjA/MQ8wDQYD
VQQDEwZtYXJldmExLDAqBgkqhkiG9w0BCQEWHWRnLWMyQGRvdWFuZS5maW5hbmNl
cy5nb3V2LmZyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/ySGkOtqQOaLG
1unj5shDnud0kN5KJxNm6bvdXfEr7Ihwz7bmML4eZK+AYcdeENmKCGmUiMZjpi5U
UvNMKSCA815DdeMQiCuwVFR7fYj6YqcuiPX3UrDjsbklL73yIvo0TxjZtGSG98ZR
drE+26+Q0wyYa4tEoZTu+cjL7bKV9wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHeh
T1j4fMDKs07iUYkbMWoLMkTM+eW0ONGg0Ejt6Ci++yE4tKm5Phz7bMVlq3Fu/Zcx
wI0vdbrDH0HNhP8NQxXYDGcDDquWTtI/E9IjPvxrrfoxXBn1meomyHH+ApTs2m5e
OctHYLP7TEvyqpwyQqVtw4x0gTVjQ2FD1aWjg7eM
-----END CERTIFICATE-----
```

Attention : ce fichier ne doit pas contenir la chaîne d'autorités de certification mais uniquement les données concernant votre certificat. Cela correspond à un seul bloc

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```