Agence des douanes et du revenu du Canada | Canada Customs and Revenue Agency

PASSERELLE INTERNET DES DOUANES

DOCUMENT DES EXIGENCES DEMANDÉES AUX PARTICIPANTS

Novembre 2003

Table des matières

1. Introduction

L'Agence des douanes et du revenu du Canada (ADRC) a mis au point la passerelle Internet des douanes pour permettre aux importateurs et aux courtiers des douanes d'envoyer et de recevoir sur Internet les données du SAED, du DECDOU, du SSMAEC et du STAM et a adopté l'infrastructure à clé publique (ICP) pour assurer la sécurité et l'intégrité des données transmises.

La passerelle Internet des douanes comprend :

- **L'envoi de données à l'ADRC**

Le client prépare les transactions comptables et(ou) de mainlevée. Le logiciel client met en forme les données selon la structure de message du SAED ou du EDIFACT. Les transactions sont chiffrées et signées numériquement par le logiciel ICP chez le client(voir l'Annexe E - Exigences techniques ICP/Internet "Points de recherche cible"). Les transactions sont envoyées par Internet au moyen du protocole HTTP. Les transactions sont reçues sur la passerelle Internet des douanes. À ce moment, un accusé de réception est envoyé à l'expéditeur. La transaction est déchiffrée, la signature numérique vérifiée et la transaction est soumise au SAED ou SSMAEC pour être traitée qui peut alors générer un accusé de réception ou un message d'erreur en rapport avec la transaction selon le Document des exigences demandées aux participants (DEDP).

- **La réception de données de l'ADRC**

Les applications SSMAEC et SAED traitent les données du client. La plate-forme de commerce électronique des douanes (PFCED) met en forme les données selon la structure de message du SAED ou du EDIFACT. Les transactions sont chiffrées et signées numériquement par la passerelle Internet des douanes. Les douanes placent les messages à destination de l'extérieur dans les files des clients. Périodiquement, l'application client vérifie auprès de l'ADRC s'il y a des messages. L'application client reçoit les transactions au moyen du protocole HTTP. L'application client déchiffre le fichier et vérifie la signature numérique de l'ADRC. Le message déchiffré du SAED ou du EDIFACT est présenté par le système commercial du client à des fins de traitement.

La connexion Internet supportera l'envoi et(ou) la réception des mêmes messages (les messages du SAED, DECDOU, SSMAEC et STAM) qui sont actuellement envoyés au moyen d'une ligne SAED ou d'un réseau à valeur ajoutée.

Le Document des exigences demandées aux participants (DEDP) comprend toute l'information dont a besoin un actuel client EDI des douanes pour utiliser la passerelle Internet. Les nouveaux clients, qui ne font pas encore appel aux options EDI qu'offre l'ADRC, peuvent obtenir de plus amples informations de même que des exemplaires du Document des exigences demandées aux participants à l'adresse suivante :

Gestionnaire
Unité du commerce électronique, Division des services à la clientèle
Direction de la politique et de la coordination opérationnelles, Direction générale des douanes
Agence des douanes et du revenu du Canada
15e étage, 191, avenue Laurier ouest
Ottawa (Ontario)
K1A 0L5
Téléphone : (888) 957-7224
Téléc. : (613) 952-9979
Adresse électronique : ecu.uce@ccra-adrc.gc.ca

L'ADRC permet aussi aux participants de maintenir un mode de communication secondaire dont ils peuvent se servir pour transmettre les données EDI en cas de panne ou s'ils ont des problèmes de communication pendant une période de quatre heures et plus. Si c'est votre cas, veuillez en informer l'Unité du commerce électronique lorsque vous ferez votre demande et un représentant de cette unité communiquera avec vous pour obtenir des détails, c'est-à-dire :

- le mode de communication secondaire que vous prévoyez utiliser (ligne SAED, réseau à valeur ajoutée);
- si vous participez actuellement à l'EDI, si vous gardez votre actuel profil EDI, notamment SAED, SSMAEC, STAM, DECDOU;
- les applications que vous voulez installer sur un système secondaire, c'est-à-dire STAM, SAED B3, SSMAEC;
- le format de transmission de vos données EDI, c'est-à-dire SAED ou Edifact et
- le numéro de votre boîte à lettres si vous utilisez un réseau à valeur ajoutée comme mode de communication secondaire.

Il vous demandera aussi d'informer votre fournisseur de logiciels que vous changez de mode de communication.

L'ADRC a choisi de faire appel à une autorité de certification pour délivrer les certificats ICP à ses partenaires commerciaux. L'ICP de l'ADRC s'appuie sur la suite Entrust. Les participants s'inscriront et l'ADRC leur délivrera un certificat ICP. Cependant, ils devront acheter le progiciel d'accès au certificat (Entrust Entelligence) et le guide d'installation de l'utilisateur. **Le certificat appartient à l'ADRC et ne doit être utilisé que pour faire affaire avec l'ADRC.**

Ce document comprend deux sections supplémentaires, la section 2 qui décrit l'ICP et indique la façon dont les clients peuvent s'inscrire à l'ICP de l'ADRC.

La section 3 décrit les tests que doivent exécuter les clients qui échangent actuellement des transactions électroniques avec l'ADRC dans un environnement de production. Les nouveaux clients eux doivent communiquer avec le gestionnaire de l'Unité du commercer électronique. Tous les détails de ces tests sont énoncés dans les Documents des exigences demandées aux participants que l'ADRC a déjà publiés sur les applications SAED, DECDOU, SSMAEC et STAM. La section 3 donne aussi les noms de personnes-ressources avec qui les clients peuvent communiquer s'ils ont quelque difficulté à utiliser la passerelle Internet des douanes.

L'annexe A contient un aperçu général des spécifications (protocole) techniques en rapport avec la syntaxe générale et les structures de codes utilisées pour communiquer sur Internet avec les applications du secteur commercial des douanes de l'ADRC. **Pour de plus amples informations sur ces spécifications, veuillez vous adresser au :**

Gestionnaire
Unité du commerce électronique, Division des services à la clientèle
Direction de la politique et de la coordination opérationnelles, Direction générale des douanes
Agence des douanes et du revenu du Canada
15e étage, 191, avenue Laurier ouest
Ottawa (Ontario)
K1A 0L5
Téléphone : (888) 957-7224
Téléc. : (613) 952-9979
Adresse électronique : ecu.uce@ccra-adrc.gc.ca

Il est absolument indispensable de ne communiquer ces spécifications à personne de l'extérieur. Lorsque l'ADRC fait part de ces spécifications détaillées à l'organisation, c'est à l'organisation

qu'il incombe de protéger cette information et de s'assurer qu'elle n'est transmise à personne d'autre.

Les clients qui veulent programmer la connexion Internet/ ADRC sur leur propre système doivent respecter ces spécifications qu'ils peuvent obtenir auprès de l'Unité du commerce électronique. Les clients qui font actuellement affaire avec un fournisseur de logiciels doivent déterminer avec celui-ci les exigences système et les coûts supplémentaires que suppose l'établissement de cette connexion. **Il est important de noter que cette interface de connexion doit être établie avant l'inscription à l'ICP.**

Vous trouverez ci-jointes en annexe à la fin du document l'Entente avec un organisme externe concernant la délivrance et l'utilisation de certificat(s) pour le Projet de passerelle Internet des douanes et l'Entente d'abonnement régissant la délivrance et l'utilisation de certificat(s) pour le Projet de passerelle Internet des douanes que les clients doivent remplir avant d'utiliser la passerelle Internet des douanes; la façon dont les clients peuvent se procurer le logiciel de cryptographie Entrust et les exigences techniques concernant l'ICP/ Internet.

Si vous avez des questions sur ce Document des exigences demandées aux participants, veuillez communiquer avec le gestionnaire de l'Unité du commerce électronique à l'adresse mentionnée précédemment.

2. Infrastructure à clé publique (ICP)

2.1 Qu'est-ce qu'une ICP?

Une ICP est un système automatisé qui gère la génération, la maintenance et la fourniture de clés de chiffrement et de signature numérique qui ensemble assurent :

- **La confidentialité** – Les données sont masquées et protégées, les personnes non autorisées ne pouvant ni les voir ni y avoir accès.
- **L'intégrité** – Le vérificateur d'une signature numérique peut facilement déterminer si les données signées numériquement ont été modifiées depuis leur signature.
- **L'authentification** – Les utilisateurs peuvent en toute sécurité s'identifier aux autres utilisateurs et serveurs d'un réseau sans envoyer de l'information secrète (comme des mots de passe) sur le réseau.
- **La non-répudiation** – Les utilisateurs qui ont apposé une signature numérique ne peuvent nier l'avoir fait.
- **Le contrôle de l'accès** – Seuls les utilisateurs désignés au moment du chiffrement peuvent accéder aux données lisibles.

Les deux types de clés, le chiffrement et la signature numérique, comprennent deux composants : un composant à clé publique à laquelle tous les utilisateurs ont accès et un composant à clé privée dont il faut protéger l'accès. La clé publique et les autres données d'identification sont stockées dans un certificat numérique signé numériquement par une autorité de certification (AC). La signature numérique de l'AC qui figure sur le certificat numérique lie l'identité de l'entité réceptrice à sa clé publique. Elle garantit aussi que la clé publique n'a pas été altérée.

Pour assurer un certain degré de confiance dans l'AC, il faut respecter certaines politiques et procédures, un des éléments importants étant le processus d'inscription, soit la façon dont un client est identifié et authentifié avant la délivrance d'un certificat numérique.

2.2 Processus d'inscription à l'ICP

Pour participer à ce nouveau Projet de passerelle Internet, les participants doivent s'inscrire à l'ICP de l'ADRC. Pour ce faire, tous les participants au projet doivent être adéquatement identifiés et authentifiés, respecter les modalités qui régissent l'utilisation des certificats numériques que délivre l'ADRC et acquérir le logiciel client ICP.

L'inscription se fait en ligne, sur le site Web d'inscription à l'ICP de l'ADRC, sauf en ce qui concerne la signature et l'envoi de l'Entente d'abonnement et de l'Entente avec un organisme externe. **L'employé (« le fondé de pouvoir ») qui, à la fin du processus, gérera le(s) certificat(s) numérique(s) doit faire l'inscription.**

Tous les participants doivent procéder comme suit, à la satisfaction de l'ADRC, pour participer au nouveau Projet de passerelle Internet.

Étape 1

Lorsque le fondé de pouvoir d'un client tel un courtier/ importateur des douanes (« l'organisation »), veut participer au projet, il devra examiner le Document des exigences demandées aux participants. Après quoi, il doit visiter le site Web d'inscription en ligne protégé et fournir l'information suivante pour lancer le processus :

Le fondé de pouvoir doit télécharger et remplir les ententes de l'ICP, y compris l'Entente avec un organisme externe, l'annexe de l'Entente avec un organisme externe, l'Entente d'abonnement et le Formulaire d'abonné (RC129). Vous trouverez ces documents à l'adresse suivante :
https://reg-pki-ext.ccra-adrc.gc.ca/cig/requirements.do

Entente avec un organisme externe – Ce document doit être signé par un cadre supérieur (l'autorité organisationnelle) qui est autorisé à lier l'organisation. Cette entente fait état des modalités qui régissent la participation à l'ICP de même que des responsabilités de l'organisation. Elle indique aussi le nom des personnes qui peuvent recevoir et gérer les certificats numériques.

Annexe A de l'Entente avec un organisme externe – Ce document doit être rempli par un cadre supérieur qui est autorisé à lier l'organisation. Cette annexe indique le nom des personnes qui peuvent recevoir et gérer les certificats numériques. Elle doit également comprendre le numéro d'entreprise (NE) de l'organisation ainsi que l'adresse de courriel de la personne-ressource principale.

Entente d'abonnement – Ce document doit être signé par le fondé de pouvoir sur l'Entente avec un organisme extérieur pour recevoir et gérer les certificats numériques. Cette entente fait état des modalités qui régissent la garde et l'utilisation des certificats numériques.

Formulaire d'abonné (RC129) – Ce formulaire doit être rempli par l'employé (le fondé de pouvoir) qui, à la fin du processus, gère les certificats numériques. Le fondé de pouvoir doit remplir la section 1 du formulaire RC129 (sans oublier d'y inscrire son adresse de courriel), tandis que l'autorité organisationnelle doit remplir la section 2. L'information contenue dans ce formulaire est protégée et conservée dans ADRC PPU 165 l'Infrastructure à clé publique pour les clients externes.

Une fois que les ententes susmentionnées sont remplies et signées, elles doivent être envoyées au représentant de l'ADRC. De plus, l'Entente avec un organisme externe signée par une entreprise doit être accompagnée d'une copie certifiée des règlements en matière de signature de l'entreprise ainsi qu'une copie certifiée de l'attestation de charge. Lorsqu'elles sont signées par un partenaire, elles doivent être accompagnées par une copie certifiée de la preuve d'enregistrement de nom.

Les ententes de même que les documents connexes doivent être envoyés par la poste ou par messagerie seulement à l'adresse suivante :

Gestionnaire
Unité du commerce électronique, Division des services à la clientèle
Direction de la politique et de la coordination opérationnelles, Direction générale des douanes
Agence des douanes et du revenu du Canada
15e étage, 191, avenue Laurier ouest
Ottawa (Ontario)
K1A 0L5

Téléphone : (888) 957-7224
Télécopieur : (613) 952-9979
Adresse électronique : ecu.uce@ccra-adrc.gc.ca

Lorsque le représentant de l'ADRC reçoit les documents, il vérifie s'ils sont bien remplis et communique avec le cadre supérieur qui a signé l'entente pour obtenir, s'il y a lieu, les renseignements

supplémentaires dont il a besoin pour terminer l'authentification du fondé de pouvoir et de l'organisation. Lorsque le représentant de l'ADRC estime que toutes les conditions sont remplies, il envoie un courriel au fondé de pouvoir pour l'inviter à remplir la demande de certificat numérique.

Étape 2

Note importante : Pour effectuer cette étape, il faut un navigateur Web de chiffrement à 128 bits et une connexion Internet. Pour plus de détails, consulter l'annexe E – Exigences techniques ICP/ Internet.

Le fondé de pouvoir recevra un avis par courriel lui indiquant son mot de passe d'inscription de 10 caractères qu'il devra utiliser pour accéder au site Web d'inscription protégé. Après avoir pris connaissance de l'information, ce dernier doit visiter le site Web d'inscription protégé, cliquer sur le bouton d'ouverture de session dans le menu de gauche et fournir l'information suivante pour accéder au site :

- le numéro d'entreprise (NE) de 9 chiffres attribué par l'ADRC à l'organisation;
- le mot de passe d'inscription de 10 caractères fournit dans l'avis envoyé par courriel.

Une fois sur le site, le fondé de pouvoir doit cliquer sur le bouton d'inscription initiale qui se trouve dans le menu de gauche.

A. Le fondé de pouvoir doit vérifier les éléments suivants de la page d'inscription initiale :

Information sur l'organisation

- le nom de l'organisation (dénomination sociale au complet)
- le numéro d'entreprise (NE) de neuf chiffres attribué par l'ADRC à l'organisation
- l'adresse postale de l'organisation, y compris le code postal
- l'adresse de courriel

Si l'information est exacte, le représentant n'a qu'à saisir son adresse de courriel.

B. Le fondé de pouvoir doit fournir l'information suivante sur la page de la personne-ressource :

Information personnelle

- le fondé de pouvoir (nom au complet)
- l'adresse postale (si elle est différente de celle de l'organisation)
- l'adresse de courriel
- le numéro de téléphone
- un secret personnalisé et les astuces correspondantes – il doit s'agir de quelque chose de facile à retenir, mais peu connu des autres (ces secrets personnels serviront à authentifier le fondé de pouvoir lorsqu'il retournera sur le site Web d'inscription à l'ICP de l'ADRC). **Le secret et l'astuce doivent être composés d'au moins 8 caractères.**
  Par exemple :
  - ⇒ Secret = SOCRATES
  - ⇒ Astuce = mon premier animal domestique
- le nombre d'appareils à enregistrer

C. Le fondé de pouvoir doit fournir l'information suivante sur la page de la personne-ressource :

Information sur l'appareil

- Le nom de l'appareil sur lequel résidera le profil du certificat. Le nom choisi doit être unique et explicite, généralement, il s'agit du nom de l'ordinateur.

Une fois l'information entrée adéquatement, un numéro d'inscription de 16 chiffres est généré et attribué

à chaque demande de certificat. Le système affiche ce numéro que le participant doit imprimer pour pouvoir le consulter et l'utiliser à l'avenir.

L'information saisie sur le site Web d'inscription à l'ICP de l'ADRC doit correspondre à celle des ententes remplies de l'ICP ainsi que des documents connexes.

Étape 3

Pendant que les étapes 1 et 2 sont en cours, le client peut procéder à l'acquisition et à l'installation de son logiciel de cryptographie, une transaction commerciale entre l'organisation et le fournisseur de logiciels et une condition préalable à l'inscription finale menant à l'obtention d'un certificat numérique de l'ADRC.

Pour plus de détails, veuillez consulter l'annexe D – Processus d'acquisition du logiciel Entrust.

Étape 4

Note importante : Le logiciel client de cryptographie doit être installé et fonctionnel pour que le fondé de pouvoir puisse retourner au site d'inscription à l'ICP de l'ADRC et exécuter la dernière étape menant à l'obtention du certificat numérique.

Un courriel sera envoyé après la réception de l'inscription de l'appareil. Le fondé de pouvoir trouvera dans ce courriel le lien qui le mènera vers le site d'inscription à l'ICP de l'ADRC.

Le système demandera au fondé de pouvoir de saisir le NE de l'organisation et le mot de passe d'inscription pour accéder au site.

Une fois sur le site, le fondé de pouvoir doit cliquer sur le bouton approprié qui se trouve dans le menu de gauche pour créer ou récupérer un profil.

Le NE et le nom de l'organisation s'afficheront. Le fondé de pouvoir devra saisir le numéro d'inscription de 16 chiffres de l'appareil.

Le nom de l'appareil, le nom de la personne-ressource et l'astuce s'afficheront. Le fondé de pouvoir n'aura qu'à saisir le secret (minimum de 8 caractères).

Une fois le fondé de pouvoir identifié, le processus automatisé de délivrance de certificat est lancé et un profil client est créé dans le système utilisé pour accéder au site Web. Ce profil peut par la suite être transféré à l'appareil cible (système) qui exécutera les transactions de l'ADRC comme le CADEX, le Système de déclaration douanière, le SSMAEC, le STAM, le secteur maritime et le PAD.

2.3 Révocation des certificats

Dans certaines circonstances, l'organisation doit immédiatement demander à l'ADRC de révoquer ses certificats, notamment si :

a) le mot de passe, le jeton ou les clés privées de l'abonné ont été ou sont soupçonnés d'avoir été compromis ou non sécuritaires de quelque façon;
b) un renseignement contenu dans un certificat ou les renseignements d'identité ou d'identification ont été modifiés ou altérés ou deviennent pour toute autre raison inexacts ou incomplets;
c) l'appareil contenant le certificat est perdu ou volé, cesse d'être utilisé ou d'être autorisé en vue de l'utilisation dans le Projet de passerelle Internet des douanes.

La demande de révocation du certificat doit être envoyée au représentant du service à la clientèle de l'ADRC à l'aide d'un courriel signé numériquement. Si ce n'est pas possible, le fondé de pouvoir doit communiquera par téléphone avec le représentant du service à la clientèle de l'ADRC qui, avant de révoquer le certificat, communique avec le cadre supérieur afin de vérifier l'identité et l'authentification du fondé de pouvoir.

L'organisation peut demander un nouveau certificat de la façon indiquée à la section 2.2.

2.4 Récupération d'un certificat

Pour assurer un climat de confiance, l'AC met périodiquement à jour les clés et les profils, et ce, automatiquement avec peu ou pas d'intervention de l'utilisateur. Cependant, dans certaines circonstances, l'abonné doit demander et exécuter une mise à jour manuelle ou forcée, particulièrement en cas de :

a) perte ou d'oubli du mot de passe;
b) corruption ou de suppression de profil (généralement à cause d'une panne matérielle ou logicielle);
c) suppression accidentelle.

Dans de tels cas, le fondé de pouvoir devra retourner sur le site d'inscription à l'ICP et sélectionner l'option de récupération au lieu de l'option de création.

Le système demandera au fondé de pouvoir de saisir le NE et le mot de passe d'inscription pour accéder au site Web d'inscription à l'ICP. Le fondé de pouvoir n'a qu'à suivre les étapes énumérées à l'étape 4 de la section 2.2 (processus d'inscription à l'ICP). Une fois le fondé de pouvoir identifié, le processus automatisé de récupération de clés est lancé et le fondé de pouvoir entre, sur demande, un nouveau nom de profil et un nouveau mot de passe.

3.0 Tests exécutés par le client

3.1 Introduction

Vous trouverez dans cette section de l'information sur les différents tests qu'il faut exécuter pour transmettre des données à l'Agence des douanes et du revenu du Canada (ADRC) par Internet. **Il convient de noter que ces exigences s'adressent spécifiquement aux clients qui se trouvent actuellement dans l'environnement de production.** Vous trouverez ci-dessous la définition de tous les tests de communication en rapport avec chaque application EDI des douanes.

Les nouveaux clients qui transmettent des données sur Internet doivent se conformer aux modalités énoncées dans le Document des exigences demandées aux participants sur le système EDI spécifique que tous les participants doivent consulter et dont ils doivent tenir compte dans leur plan de développement. Vous pouvez obtenir un exemplaire du Document des exigences demandées aux participants sur l'application EDI qui vous intéresse à l'adresse suivante :

Gestionnaire
Unité du commerce électronique, Division des services à la clientèle
Direction de la politique et de la coordination opérationnelles, Direction générale des douanes
Agence des douanes et du revenu du Canada
15e étage, 191, avenue Laurier ouest
Ottawa (Ontario)
K1A 0L5
Téléphone : (888) 957-7224
Téléc. : (613) 952-9979
Adresse électronique : ecu.uce@ccra-adrc.gc.ca

3.2 Tests

3.2.1 Tests internes exécutés par le client

Les participants sont responsables d'exécuter tous les tests internes en rapport avec les composantes de leur interface Internet. Ceci comprend l'essai

- de tous les codes d'application personnalisés utilisés pour traiter les enregistrements d'entrée et de sortie;
- de tous les sous-programmes de traitement des erreurs et de production de rapports sur les anomalies et
- du traitement des accusés de réception échangés avec l'ADRC.

3.2.2 Essai du réseau du fournisseur de services Internet

C'est aux participants, de concert avec leur fournisseur de services Internet (FSI), qu'il incombe de tester le réseau. Le FSI doit fournir aux clients le soutien direct dont ils ont besoin pour cette phase à laquelle l'ADRC ne participe pas. Lorsque les clients ont établi une bonne communication avec leur fournisseur de services, ils informent le représentant du service à la clientèle de l'Unité du commerce électronique qu'ils sont prêts à établir la connexion avec l'ADRC.

3.2.3 Services de communication Internet/ client

La responsabilité de l'interface avec le fournisseur de services Internet (FSI) revient au fournisseur de services, votre FSI. Ainsi, tous les problèmes reliés à la connexion et(ou) à la transmission des données sur Internet doivent être résolus par le fournisseur de réseau.

Voici le processus de base qu'il faut suivre pour établir une connexion Internet :

- déterminer le fournisseur de services Internet auquel votre organisation fera appel pour établir l'interface avec l'ADRC
- informer votre FSI que vous transmettrez des messages chiffrés à l'ADRC
- établir une interface de communication avec le matériel et le logiciel appropriés
- acquérir et installer le logiciel Entrust
- configurer et tester toutes les composantes et tous les programmes d'interface avec le FSI
- si votre entreprise a déjà un FSI, vous devez satisfaire aux exigences énoncées à l'annexe D. De plus, vous devez installer le programme de chiffrement et signer une entente entre partenaires commerciaux avec l'ADRC. Ensuite, vous pourrez transmettre des données.

Vous devez vous assurer que vous pouvez recevoir un accusé de réception de l'ADRC chaque fois que vous lui transmettez un message.

3.3 Jeux d'essai : Applications EDI de douanes

Selon les applications, vous devez exécuter les jeux d'essai avant de transmettre des données à l'ADRC sur Internet. Veuillez communiquer avec l'Unité du commerce électronique au (888) 957-7224 pour fixer la date des essais. **Les clients devront confirmer qu'ils ont reçu un accusé de réception des données transmises de l'ADRC dans le cas de tous les jeux d'essai transmis.**

3.3.1 SAED et DECDOU

a) Transmettre cinq entrées que vous utilisez généralement en mode production pour tester l'acceptation de vos entrées et la génération du relevé comptable K84

b) Consulter les fichiers des taux de change et de classification pour vérifier si la bonne information est transmise.

c) Remettre au responsable des tests de l'Unité du commerce électronique quatre numéros de transaction inutilisés qui serviront à la création d'enregistrements de mainlevée pour tester la génération du Rapport sur la transmission des avis de mainlevée du SAED et des messages de transmission automatique des avis de mainlevée du DECDOU et du Rapport sur la mainlevée dont la déclaration de confirmation est en souffrance du SAED et du DECDOU.

d) Facultatif – Fournir au responsable des tests de l'Unité du commerce électronique un ou une série de numéros de classification pour tester le téléchargement de la classification.

3.3.2 SSMAEC

a) Transmettre un message SEA original. Les données permettant de faire l'appréciation suivront.
Changer la transaction.
Annuler la transaction.

b) Transmettre une transaction originale MDM avec les données permettant de faire l'appréciation.
Changer la transaction.

c) Transmettre une transaction originale MDM sans les données permettant de faire l'appréciation. Le responsable des tests créera un Y51 et communiquera avec le client pour vérifier s'il a reçu un code numéro 6 ou le texte.

d) Transmettre une transaction MDM originale avec les données permettant de faire l'appréciation. Le responsable des tests examinera la transaction et communiquera avec le client pour vérifier s'il a reçu un code numéro 5 ou le texte.

e) Transmettre une transaction MDM avec les données permettant de faire l'appréciation et trois factures (bons de commande) portant chacune cinq lignes de description.

3.3.3 Système de transmission des avis de mainlevée

3.3.3.1 Système automatique de transmission des avis de mainlevée

Fournir cinq numéros de transaction et cinq numéros de contrôle du fret (NCF). Le responsable des tests créera cinq enregistrements de mainlevée pour vérifier si le client reçoit les messages du Système automatique de transmission des avis de mainlevée.

3.3.3.2 Arrivées

a) Transmettre une arrivée (631) avec un NCF (fourni par le client) et le bureau de mainlevée 0677 pour vérifier si le client reçoit un code d'erreur 6, indiquant que le bureau de douanes est incorrect.

b) Transmettre une arrivée (631) avec un numéro de transaction (fourni par le client) et le bureau de mainlevée 0395 pour tester si le client reçoit un code d'erreur 11, indiquant une arrivée par numéro de transaction interdite.

c) Transmettre une arrivée (631) avec un NCF (fourni par le client) et le bureau de mainlevée 0395 et une date future pour vérifier si le client reçoit un code d'erreur 4, indiquant que la date d'arrivée est future.

d) Transmettre une arrivée (631) avec un NCF (fourni par le client), le bureau de mainlevée 0398 et une date courante pour vérifier si le client reçoit un code 4 du GIS, indiquant que les marchandises sont dédouanées.

3.3.3.3 Consultation de l'état

a) Transmettre une transaction de consultation de l'état (998) avec un NCF (fourni par le client), le bureau de mainlevée 0395 et une date courante pour vérifier si le client reçoit un code GIS (accepté, en attente des marchandises) ou un code 4 (marchandises dédouanées) selon le type de mainlevée.

b) Transmettre les transactions de consultation de l'état (998) avec un numéro de transaction (fourni par le client), le bureau de mainlevée 0395 et la date courante pour vérifier si le client reçoit un code 02, indiquant que le numéro de transaction est introuvable.

c) Transmettre une transaction de consultation de l'état (998) avec un NCF (fourni par le client), le bureau de mainlevée 0395 et une date future pour vérifier si le client reçoit un code d'erreur 01, indiquant que le NCF est introuvable.

d) Transmettre une transaction de consultation de l'état (998) avec un numéro de transaction (fourni par le client), le bureau de mainlevée 0667 et la date courante pour vérifier si le client reçoit un code GIS 9 (accepté, en attente des marchandises) ou un code 4 (marchandises dédouanées) peu importe le code de bureau incorrect.

3.4 Lignes de communication

3.4.1 Signalement et résolution des problèmes

À chaque participant au projet est affecté un représentant du service à la clientèle de l'Unité du commerce électronique, la première personne avec qui le client devra communiquer concernant tous les problèmes et toutes les demandes de renseignements sur la transmission de données sur Internet, sauf durant la phase d'essai du réseau initial.

Selon la nature et les circonstances du problème, le représentant du service à la clientèle détermine si le problème est en rapport avec la structure de communication de l'ADRC. Dans la négative, on vous demandera de communiquer avec votre FSI. En ce qui concerne les problèmes techniques ou en rapport avec les applications, le représentant du service à la clientèle les affectera au secteur approprié au sein de la Direction générale de la technologie de l'information de l'ADRC.

Voici la procédure à suivre pour signaler un problème à différentes étapes du projet.

Essai initial du réseau du FSI
Les participants font part des problèmes de réseau/ communication directement au fournisseur de services Internet de la façon indiquée par le fournisseur. Les problèmes sérieux et(ou) permanents doivent être signalés au représentant du service à la clientèle.

Essai de l'application
Les participants qui rencontrent des problèmes durant cette phase communiquent avec leur représentant du service à la clientèle qui examinera le problème et s'il est incapable de le résoudre, l'entrera dans le Système de gestion des problèmes de l'ADRC pour qu'il soit affecté à la section de soutien qui convient. La Division des services à la clientèle de l'ADRC assumera l'entière responsabilité du suivi et de son report à un échelon supérieur à des fins d'essai et de production.

Production Internet
Les problèmes de réseau doivent être signalés au FSI pour qu'il en détermine d'abord la cause et trouve ensuite la solution. **Veuillez signaler tous les problèmes opérationnels ou en rapport avec l'application à l'Unité du commerce électronique au (888) 957-7224 (adresse électronique : ecu.uce@ccra-adrc.gc.ca) pour obtenir rapidement l'aide d'un représentant du service à la clientèle.**

Implantation
Lorsque tous les tests ont été exécutés avec succès, le client fixe une date d'implantation dans l'environnement de production avec le représentant du service à la clientèle qui lui a été affecté.

Annexe A: Spécifications Techniques (Protocole)

Spécification du protocole de services de commerce électronique

Applications commerciales des douanes - Transport protégé des fichiers via l'Internet au moyen du protocole de transfert hypertexte (HTTP) et des projets de normes EDIINT

Historique des révisions

Numéro de la révision	Résumé de la révision
00.0327	Document original
00.0606	• Le tableau des définitions d'en-têtes de la section 7.1, qui fait référence à la version du protocole HTTP dans la commande HTTP, indiquait précédemment le réglage " HTTP/1.1 ", avec renvoi à la spécification RFC 2616. **Ce réglage a été remplacé par " HTTP/1.0 " et renvoie maintenant à la spécification RFC 1945.** • La section 7.10 définit le code de retour 204 comme indiquant qu'il n'y a pas de données en file d'attente à l'ordinateur hôte pour livraison. **Ce code a été remplacé par le code de retour 205.** • La section 7.9 comprend une nouvelle illustration montrant le téléchargement de messages multiples à partir de la fille d'attente des réponses. • La section 7.10 illustre maintenant le format d'un message indiquant qu'il n'y a pas de données en file d'attente pour le destinataire.
00.0703	• La section 7.10 définit le code de retour 204 comme indiquant qu'il n'y a pas de données en file d'attente à l'ordinateur hôte pour livraison. Dans la révision 0606, ce code a été remplacé par le code de retour 205. Par suite des modifications apportées au serveur HTTP, c'est le **code de retour 204** qui est renvoyé pour indiquer l'absence de données en file d'attente. Par conséquent, la spécification originale demeure en vigueur. • Toutes les adresses URI correspondent maintenant à l'environnement OPS. • De plus, en raison de la mémorisation par bloc obligatoire du protocole HTTP 1.1 et d'autres caractéristiques non pertinentes pour la mise en œuvre de l'ADRC, le protocole HTTP 1.0 sera considéré comme la spécification de référence pour la mise en œuvre. Ainsi, tous les renvois au protocole HTTP 1.1 ont été modifiés pour tenir compte de ce changement. L'Annexe A, Code source CPP, a été supprimée.

Table des matières

1. Portée

Cette spécification décrit la syntaxe et les construits de codage généraux qui sont nécessaires pour communiquer sur l'Internet avec les Applications commerciales des douanes de l'Agence des douanes et du revenu du Canada en utilisant :

- la norme de syntaxe de message cryptographique PKCS#7 avec
- les projets de normes proposés pour l'ÉDI sur l'Internet et
- le protocole HTTP (Hypertext Transfer Protocol/protocole de transfert hypertexte).

La prise en charge de la norme PKCS#7 est assurée par l'utilisation de la boîte à outils Entrust Toolkit d'Entrust Technologies.

Bien que le contenu de cette spécification se veuille non spécifique, dans les passages où la généralisation aurait nui à la description (par ex. : les construits de codage), on a utilisé :

- le langage informatique C++
- " CADEX " comme nom de l'application.

2. Références

PKCS # 7	RSA Laboratories, PKCS #7 Cryptographic Message Syntax Standard, Version 1.5, novembre 1993
RFC 1945	Hypertext Transfer Protocol, HTTP1.0 T. Berners-Lee et al; mai 1996
RFC 822	Standard For The Format of ARPA Internet Text Messages, David H. Crocker, Dept of EE, University of Delaware, août 1982
RFC 1521	MIME (Multipurpose Internet Mail Extensions Part One, - Standards Track N. Borenstien, Bellcore, N. Freed, Innosoft, septembre 1993
Draft-ietf-ediint-req-08.txt	Requirements for Inter-operable Internet EDI - Draft Proposal - T Harding, Cyclone Software, R. Drummond, Drummond Group, C. Shih, Gartner Group, septembre 1999
Draft-ietf-as1-11.txt	Mime-based Secure EDI - Draft Proposal - T Harding, Cyclone Software, R. Drummond, Drummond Group, C. Shih, Gartner Group, septembre 1999
Draft-ietf-ediint-as2-06.txt	HTTP Transport for Secure EDI – Draft Proposal – D. Moberg, D. Brooks, R. Drummond, octobre 1999
RFC 1847	Security Multiparts for MIME : J. Galvin, S. Murphy, Trusted Information Systems, S. Crocker, CyberCash, Inc., N. Freed, Innosoft International, Inc., octobre 1995
RFC 2298	An Extensible Message Format for Message Disposition Notification : R. Fajman, National Institutes of Health, mars 1998
RFC 1848	MIME Object Security Services- Standards Track, octobre 1995
Software Release 5.01	Entrust/Toolkit C++ Edition - Programmers Guide/Programmers Reference, Software Release 5.01

3. Définitions

CRLF	" Dans ce document, le terme CRLF désigne la séquence des deux caractères ASCII CR (13) et LF (10) qui, ensemble et dans cet ordre, dénotent une fin de ligne dans le courrier RFC822. "[1]

[1] RFC1521, section 2.

4. Symboles et abréviations

Abréviation	Définition
HTTP	Hypertext Transfer Protocol/Protocole de transfert hypertexte
IETF	Internet Engineering Task Force
MIME	Multipurpose Internet Mail Extensions
S/MIME	Secure Multipurpose Internet Mail Extensions
PKCS	Public Key Cryptography Standards/Normes de cryptographie à clé publique
ADRC	Agence des douanes et du revenu du Canada
RFC	Request for Comments/Appel de commentaires
URI	Uniform Resource Identifier
MDN	Message Delivery Notification/Avis de livraison de message
MIC	Message Integrity Check/Vérification de l'intégrité du message

Symbole	Définition
	Aucun symbole n'est défini ou utilisé dans le présent document.

5. Aperçu général

Ce document est conçu comme une spécification technique. L'on suppose donc que le lecteur est familiarisé avec les aspects techniques de :

- la norme du protocole HTTP (Hypertext Transfer Protocol)
- la norme MIME (Multipurpose Internet Mail Extensions) et son pendant sécurisé (S/MIME)
- la terminologie du service X.500 et du protocole LDAP (Lightweight Directory Access Protocol)
- la norme de cryptographie à clé publique (PKCS) et
- la messagerie Internet en général.

Le lecteur est également encouragé à se procurer et à lire les normes utilisées et citées dans cette spécification. On peut se procurer les documents RFC et les projets de normes de l'IETF sur le site Web www.ietf.org/home.html, et la documentation RSA sur le site Web www.rsasecurity.com/index.html. Les renseignements relatifs à Entrust (y compris les boîtes à outils et la documentation connexe) sont accessibles sur le site Web www.entrust.com.

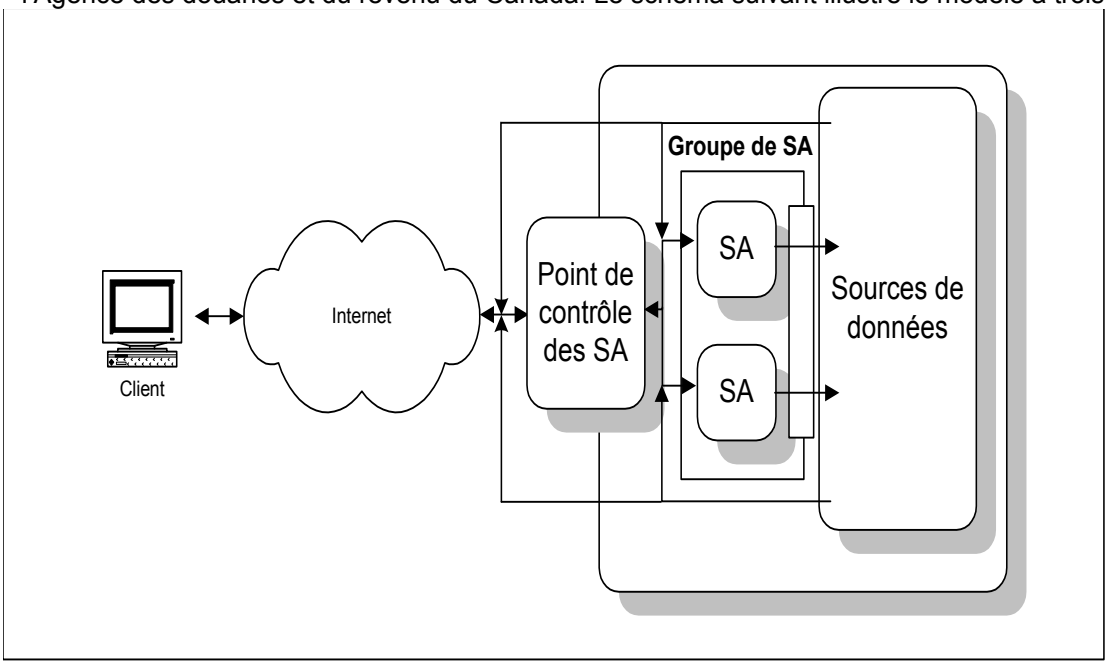
Renvois par des tiers à la présente spécification : cette spécification ne vise pas à prescrire ou à imposer les formats ou les algorithmes internes, les fonctions système spécifiques et/ou les caractéristiques d'une interface utilisateur servant à consulter, à manipuler ou à créer les messages Internet définis.

Ces spécifications sont fournies telles quelles sans garantie expresse ou implicite.

6. Environnement de l'Agence des douanes et du revenu du Canada

6.1 Le modèle à trois niveaux

L'architecture dans laquelle s'effectuent les transferts de fichiers protégés entre les clients et l'Agence des douanes et du revenu du Canada correspond au modèle dit à trois niveaux. Le premier niveau représente l'application du client, dont les spécifications sont décrites ici. Le deuxième niveau correspond aux serveurs d'application (SA) et le troisième niveau correspond à la source ou aux sources de données. Les deuxième et troisième niveaux résident dans l'infrastructure de réseau de l'Agence des douanes et du revenu du Canada. Le schéma suivant illustre le modèle à trois niveaux :



6.2 Le deuxième niveau - le serveur d'application

Les plates-formes informatiques qui correspondent au deuxième niveau sont les serveurs d'application (SA). Ces serveurs ont pour fonction de mettre en œuvre la logique opérationnelle d'une application particulière. Le nombre de serveurs d'application situés au deuxième niveau peut être modifié dynamiquement (par groupage) en réponse à une charge de travail fluctuante. On désigne alors un serveur d'application devant servir de point de contrôle, ou point de convergence pour les demandes des clients. Le point de contrôle des SA (PCSA) achemine la demande au SA chargé d'y répondre. À noter que la réponse n'est pas (nécessairement) acheminée au client via le point de contrôle, ce qui permet des gains de performance importants pour le demandeur.

6.2.1 L'adressage à l'intérieur du deuxième niveau

L'adressage à l'intérieur du deuxième niveau est représenté à la manière traditionnelle du protocole Internet par une adresse de l'hôte/adresse de données. Un exemple de cet appariement pourrait être :

serveur.adrc.gc.ca /adresse/ contrôle.des_serveurs

où

serveur.adrc.gc.ca	Représente l'adresse de l'hôte, c.-à-d. l'adresse de destination de la demande. Dans l'illustration précédente, cette adresse serait celle du point de contrôle des serveurs d'application.
/adresse/des.données	Correspond à l'adresse des données. À

noter que, dans notre illustration, l'adresse des données pourrait être celle du point de contrôle des serveurs d'application (ou PCSA) ou encore, le PCSA pourrait déterminer qu'un autre SA du groupe correspond à cette adresse de données et acheminer la demande en conséquence.

6.3 Les adresses spécifiques de niveau 2 au sein de l'ADRC

Pour l'environnement OPS :

On trouvera, à la section 7.1 - L'en-tête du message, des renseignements supplémentaires sur l'adressage.

6.4 Le troisième niveau - la source de données

Le niveau trois correspond à la source ou aux sources de données de l'application, qui peuvent inclure des entités comme des bases de données ou des systèmes de messagerie conçus pour acheminer les demandes des clients visant d'anciennes applications. Le déplacement des données à destination et en provenance du niveau trois incombe aux entités du niveau deux.

7. Définitions lexicales

La section suivante permettra au lecteur de se familiariser avec les définitions lexicales des fichiers de données qui seront transmis à l'Agence des douanes et du revenu du Canada et reçus par l'Agence. Toutes les définitions sont basées sur des normes internationales (ou des propositions de normes) de l'Organisation internationale de normalisation (ISO) ou de l'Internet Engineering Task Force (IETF). Ainsi, tout système qui traite des données en fonction de ces spécifications peut bénéficier de tous les avantages des " normes ouvertes ". Le texte renvoie aux normes pertinentes lorsqu'il y a lieu.

On peut également utiliser ces normes comme base de communication avec d'autres systèmes qui suivent les normes de formatage de la messagerie textuelle Internet. Au bout du compte, les communications réseau décrites dans le présent document sont conformes à l'avant-projet de norme Internet proposée pour :

- L'ÉDI Internet interopérable, décrit dans le document " draft-ietf-ediint-req-08.txt ";
- L'ÉDI sécurisé basé sur MIME, décrit dans le document " draft-ietf-ediint-as1-11.txt ";
- Le transport HTTP pour l'ÉDI sécurisé, décrit dans le document " draft-ietf-ediint-as2-06.txt ";

Dans la présente section, un message Internet est défini comme comportant deux éléments distincts : l'en-tête et le corps du message. Le terme message désigne l'ensemble de l'entité, à savoir l'en-tête et toutes les parties du corps du message.

Au niveau le plus élevé, l'en-tête du message peut être défini comme étant composé de champs individuels représentant de l'information qui n'est requise qu'une seule fois à l'intérieur du message.

Le corps du message Internet est défini officiellement comme étant " simplement une séquence de lignes contenant des caractères ASCII ".[2] Cette définition suffira pour l'instant, mais, à mesure que l'on avancera dans cette section, on en viendra à une définition plus sophistiquée du corps du message qui répondra aux exigences de cette spécification.

La définition de l'en-tête et du corps du message se poursuit dans le reste de cette section.

7.1 L'en-tête du message

Dans le cadre de cette spécification, les documents RFC 822 et 1945 définissent l'en-tête du message. Un message Internet est illustré et défini ci-dessous :

L'en-tête de message EDIINT

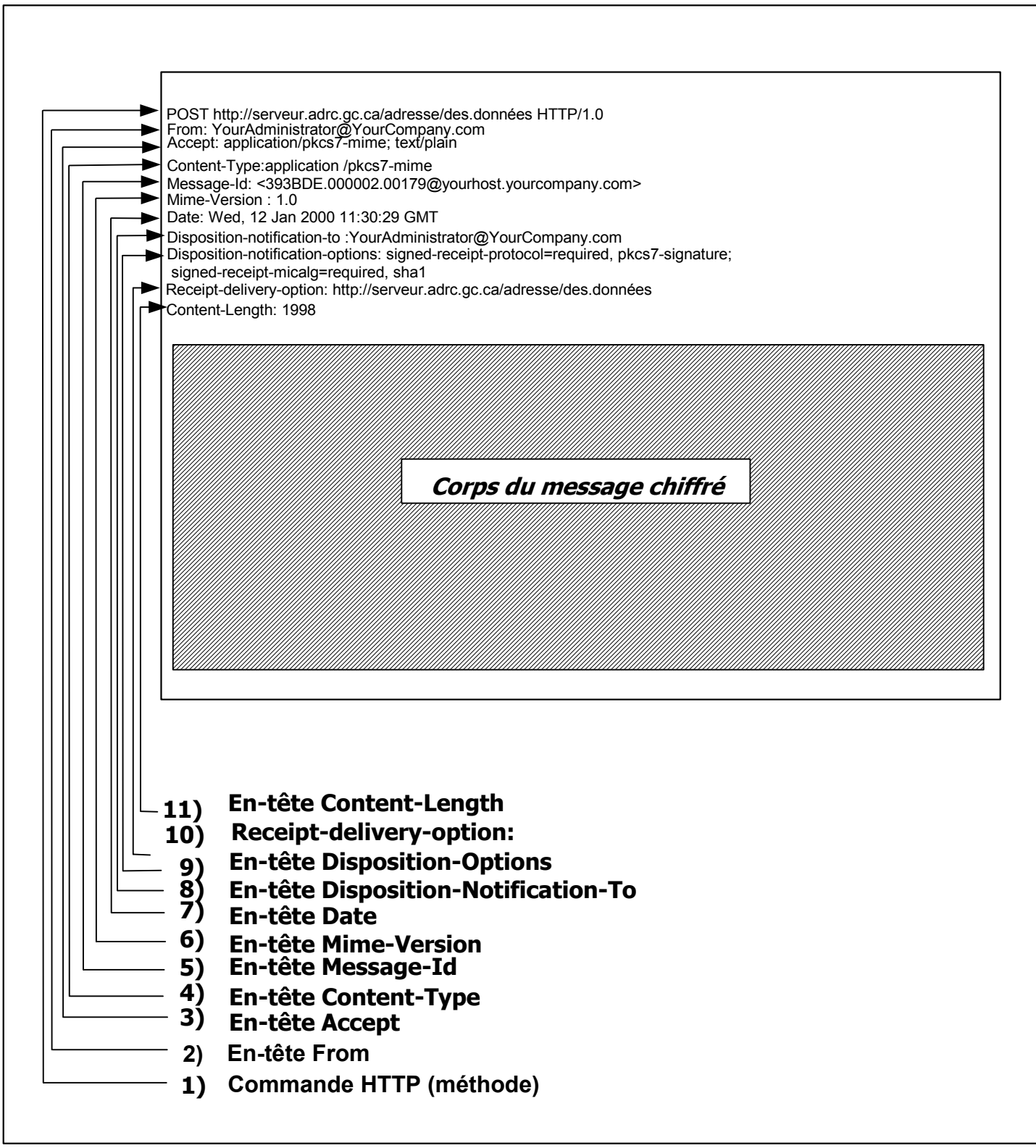
Nom du champ de l'en-tête de demande	Sous-champ	Description	Référence
HTTP Command[3]	POST	ndique au serveur de destination que tout le corps du message devrait être acheminé en tant que données à l'adresse de données indiquée.	RFC1945, section 5 / 8.3
	data address	L'adresse URI d'une ressource résidant à l'Agence des douanes et du revenu du Canada. Il s'agit d'une adresse requise fournie au client par l'ADRC.	RFC1945, section 5.1.2
	HTTP Version	Actuellement réglé à " HTTP/1.0 "	RFC1945, section 5.1
From	Aucun	Contient une adresse de courrier	RFC1945,

[2] RFC 822, section 3.1

[3] dont les sous-champs sont délimités par le caractère espace (0x20).

Nom du champ de l'en-tête de demande	Sous-champ	Description	Référence
		électronique Internet représentant l'administrateur système du client.	section 10.8
Message-ID	Aucun	Un numéro de séquence unique associé à l'échange.	
Mime-Version	Aucun	Actuellement réglé à " 1.0 "	RFC1945, section D.2.7
Date	Aucun	Date/heure de génération du message. Doit être exprimée en temps universel (GMT/Greenwich Mean Time)	RFC1945, section 10.6
Accept	Aucun	Sert à spécifier les types de supports acceptables pour les réponses. Au minimum, cette valeur doit être définie comme " application/pkcs7-mime; text/plain "	RFC1945, section D.2.1
Content-Type		Sert à spécifier le type de support du corps du message envoyé au destinataire. Doit être réglé à " application/pkcs7-mime ".	Draft-ietf-ediint-req-08
Disposition-Notification-to	Aucun	Voir la section 7.7 - Avis de livraison de message et boucle de message sécurisée.	Draft-ietf-ediint-as1-11
Disposition-Notification-Options	Aucun	Voir la section 7.7 - Avis de livraison de message et boucle de message sécurisée.	Draft-ietf-ediint-as1-11
Receipt-Delivery-Option	Aucun	Voir la section 7.7 - Avis de livraison de message et boucle de message sécurisée.	Draft-ietf-ediint-as2-06
Content-Length	Aucun	Spécifie la longueur du corps du message en décimale.	RFC1945, section 10.4
Ligne " nulle "	Aucun	Une paire CRLF indiquant la fin de l'en-tête du message.	RFC822, section 3.1

En voici un exemple :



Notes :

- À l'exception du champ d'en-tête " HTTP Command ", tous les champs d'en-tête délimitent le nom du champ d'en-tête avec sa valeur au moyen du caractère deux points. Par exemple :

  Content-Type: application/pkcs7-mime;
- Dans l'exemple ci-dessus, toutes les entrées comprises dans l'en-tête du message se terminent par une paire CRLF.

7.2 Le corps du message

Dans le cadre de cette spécification, les documents RFC 822, 1521 et le projet de norme EDI-INT définissent le corps du message Internet ainsi que la granularité de la définition. En d'autres termes, le document RFC 822 définit le message Internet à son niveau le plus élevé (l'en-tête seulement), tandis que le projet de norme EDI-INT définit les caractéristiques spécifiques des messages dont les types de contenu (content-types) sont " multipartie/signé " (multipart/signed).

Dans le document RFC 1521, la spécification d'un champ type de contenu multipartie dans un en-tête de message indique que le corps du message contiendra une ou plusieurs parties, dont chacune sera précédée par un délimiteur d'encapsulation (qui est lui-même précédé et suivi par une paire CRLF). En outre, la dernière partie du corps du message sera suivie d'un délimiteur de fermeture. Le délimiteur de corps de message est expliqué de façon plus détaillée dans les sections suivantes.

Une entrée de corps de message (après le délimiteur d'encapsulation) est elle-même constituée d'une zone d'en-tête, d'une ligne vide et d'une zone " corps ". Ainsi, le corps MIME est sémantiquement similaire au format d'en-tête de message décrit dans le document RFC 822. En voici un exemple :

```
Content-Type: application/edi-consent
Content-Length: 8086

... contents of EDI Transaction ...
```

Le projet de norme EDI-INT précise que chaque entrée de corps de message définie par le type de support " multipart/signed " (multipartie/signé) devrait contenir deux parties, la première ayant le type de contenu " application/<EDI standard> " et la seconde le type de contenu " application/pkcs7-signature ".

Notes :

- Tous les champs d'en-tête délimitent le nom du champ d'en-tête avec sa valeur au moyen du caractère deux points. Par exemple :

  Content-Type: application/edi-consent;
- Les définitions de paramètres sont délimitées au moyen du caractère point virgule (;)
- Dans l'exemple ci-dessus, toutes les entrées contenues dans l'en-tête du message se terminent par une paire CRLF.

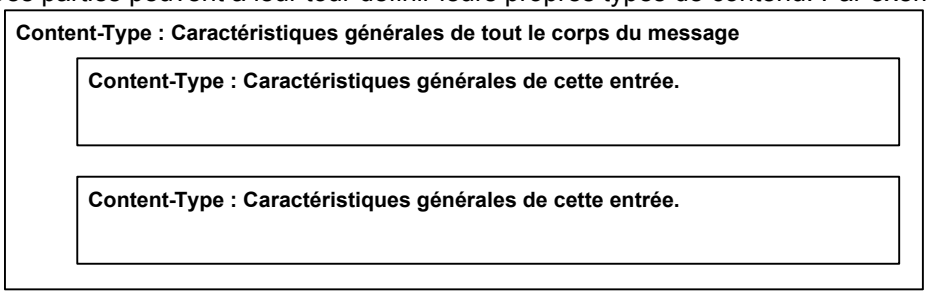
Mise en garde à l'intention des réalisateurs	Dans cette dernière section, de nombreuses données sont présentées de façon apparemment statique. Soulignons que ce ***n'est pas*** le cas. Les en-têtes HTTP et leur contenu pourraient changer avec le temps par suite de changements système ou pour améliorer l'efficience. Par conséquent, il est recommandé au lecteur d'implémenter les zones de données précédentes de manière à ce qu'elles puissent être dynamiquement modifiées (c.-à-d. sans recompiler le programme).

7.3 Le type de contenu multipartie

Jusqu'ici, nous avons défini le message Internet comme étant composé de deux parties : l'en-tête et le corps. Cependant, pour répondre aux besoins de la spécification et permettre le transport de fichiers chiffrés à l'intérieur d'un message Internet, il faut implémenter un corps de message plus sophistiqué.

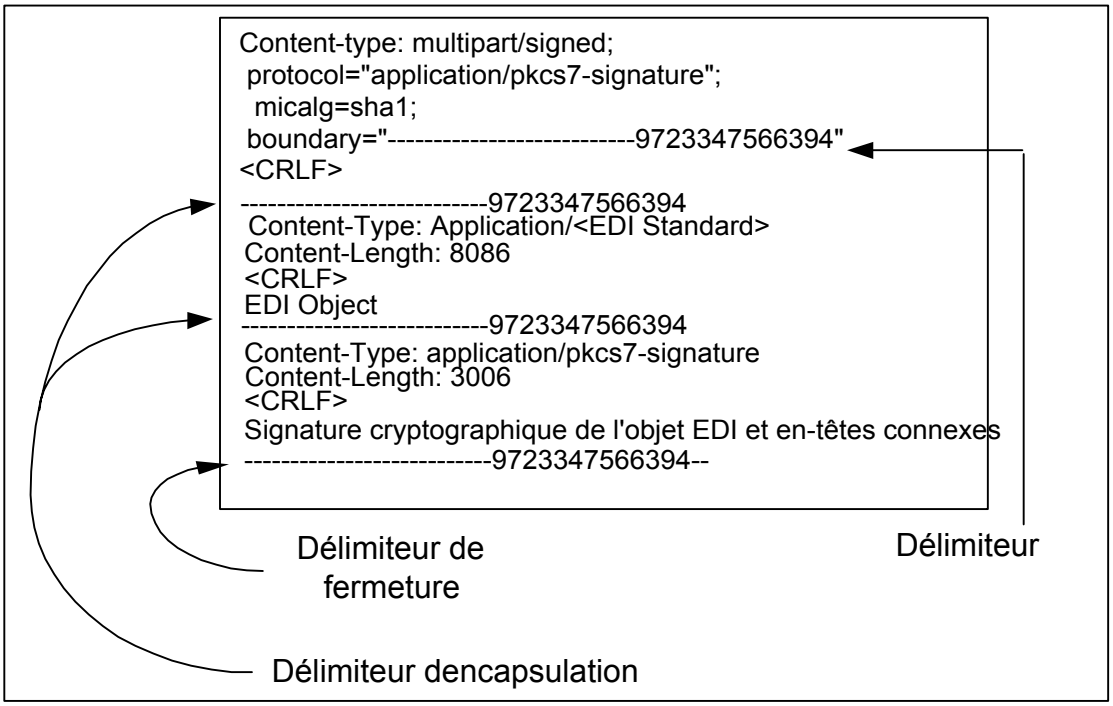
Ce corps de message raffiné est appelé corps de message multipartie et il est défini dans le cadre de la spécification Multipurpose Internet Mail Specification ou MIME. La spécification MIME est incluse dans le document RFC 1521[4] de l'IETF. Les documents RFC[5] subséquents définissent la variante sécurisée de MIME.

Cependant, pour être plus précis, la spécification RFC1521 (à partir de la section 7.2), indique, dans le cas où de multiples parties doivent être transmises à l'intérieur d'un seul message, que le type de contenu " multipart " doit apparaître en tant que champ d'en-tête de demande dans l'en-tête du message. Le premier en-tête de type de contenu définit les caractéristiques générales des parties suivantes. Ces parties peuvent à leur tour définir leurs propres types de contenu. Par exemple :



Un champ d'en-tête de demande type de contenu peut aussi définir un sous-champ appelé le champ " boundary " (délimiteur).

C'est le champ " boundary " qui sert à délimiter les différentes parties du corps du message Internet. Dans l'usage, le champ délimiteur est appelé " encapsulation boundary " (délimiteur d'encapsulation), car avant d'être utilisé, il est modifié par rapport à son état de définition original. La partie finale du corps du message se termine par une " closing boundary " (délimiteur de fermeture), qui est encore une fois une modification du délimiteur d'encapsulation original. En voici un exemple :



[4] L'un de plusieurs documents RFC définissant MIME, par ex. : de 2045 à 2049.

[5] Les documents RFC 2630, 2633 Secure/Mime V3 specification, RFC1847 Security Multiparts for MIME

Figure 1 Sémantique du type de contenu multipartie

L'élément **boundary** (délimiteur) est défini comme un sous-champ, ou paramètre, du champ d'en-tête de demande Content-type. Du point de vue de la norme, le délimiteur est simplement une chaîne aléatoire de caractères qui sert à " indexer " les parties du corps du message. La seule exigence obligatoire de la norme à l'égard du délimiteur est que la chaîne de caractères n'apparaisse pas à l'intérieur du corps de message qu'elle délimite.

Dans l'exemple précédent, la définition du délimiteur " boundary " est encadrée par des guillemets. Bien que la spécification n'exige pas l'utilisation de cette grammaire dans la définition du délimiteur " boundary ", elle recommande l'utilisation des guillemets pour éviter les définitions illégales du type de contenu. En fait, pour des raisons qui deviendront claires dans les paragraphes suivants, dans le cadre de cette spécification, *l'encadrement de la définition du délimiteur " boundary " au moyen de guillemets est considéré* ***obligatoire****.*

Aux termes de la spécification RFC1521, la longueur du délimiteur " boundary " ne doit pas dépasser 70 caractères.

Le délimiteur d'encapsulation (**encapsulating boundary)** est défini comme une ligne composée de deux traits d'union (" - " ou décimale 45) suivis de la ligne du délimiteur.

> " À noter que le délimiteur d'encapsulation doit apparaître au début d'une ligne, c.-à-d. après un CRLF, et que le CRLF initial est considéré comme étant joint au délimiteur d'encapsulation plutôt que faisant partie de la partie précédente. Le délimiteur doit être immédiatement suivi d'un autre CRLF et des champs d'en-tête de la partie suivante, ou de deux CRLF, auquel cas il n'y a pas de champs d'en-tête pour la partie suivante(et l'on suppose, par conséquent, que cette partie a le type de contenu " text/plain ").
>
> NOTE : Le CRLF qui précède la ligne d'encapsulation est conceptuellement reliée au délimiteur, de sorte qu'il est possible d'avoir une partie qui ne se termine pas par un CRLF (fin de ligne). Les parties du corps du message qui doivent être considérées se terminer par des fins de ligne doivent, par conséquent, avoir deux CRLF précédant la ligne d'encapsulation, le premier faisant partie de la partie précédente et le second faisant partie du délimiteur d'encapsulation. "[6]

L'élément **closing boundary** (délimiteur de fermeture), aussi appelé " distinguished delimiter ", se définit comme une ligne composée du délimiteur d'encapsulation suivi de deux traits d'union (" - " ou décimale 45). Le délimiteur de fermeture indique qu'aucune autre partie du corps du message ne suit.

7.4 La spécification S/MIME de EDI-INT : Signature et chiffrement (multipartie/signé)

En élaborant la définition générale du message MIME multipartie présentée ci-dessus, le projet de norme EDI-INT définit son message multipartie comme suit :

[6] RFC1521, section 7.2.1.

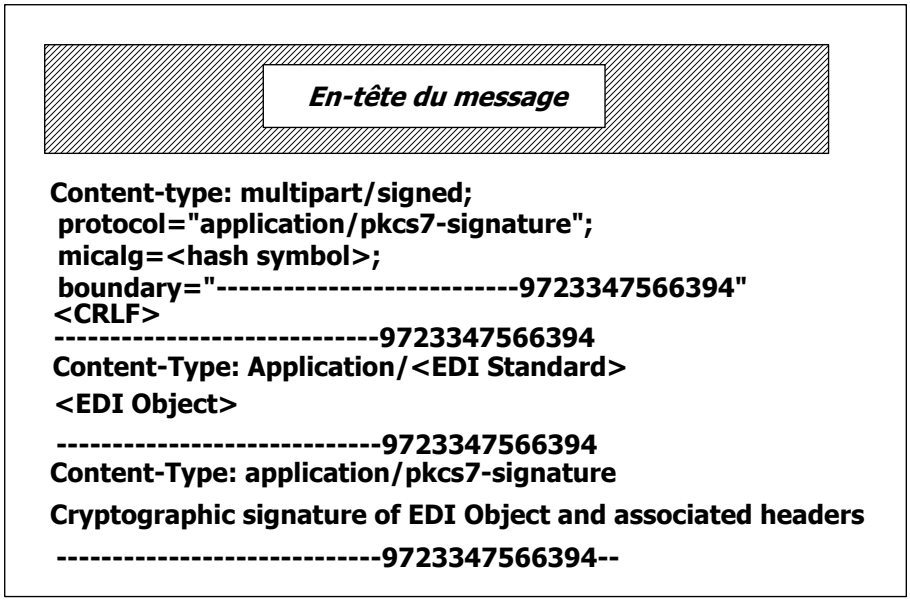


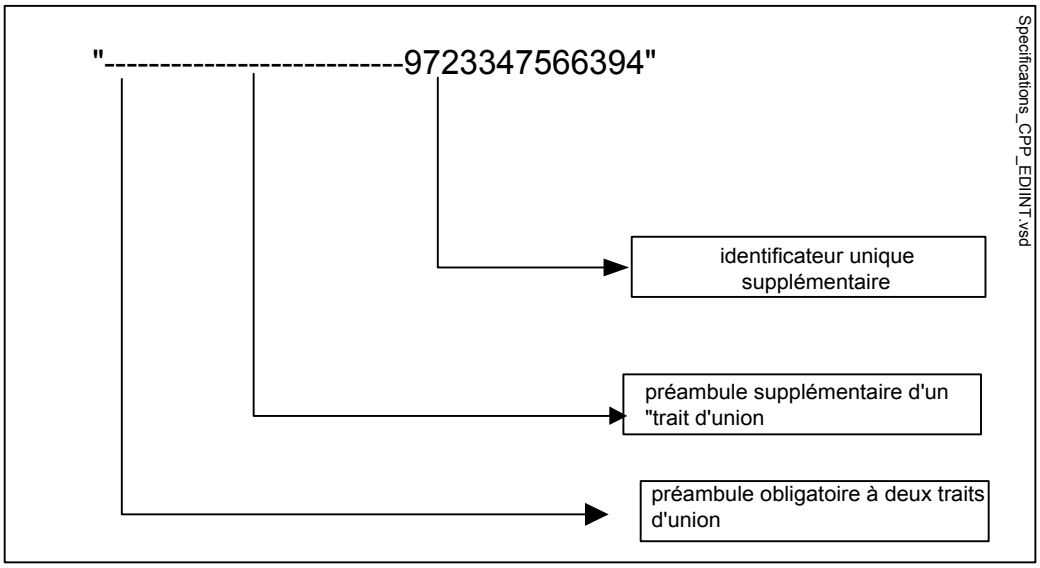
Figure 2 Corps du message EDI-INT

Le schéma précédent illustre trois parties distinctes (types de contenu) du corps d'un message :

Content-Type/Type de contenu	Sous-champ(s)	Description
Multipart/signed		Décrit les attributs s'appliquant à l'ensemble du corps du message.
	Protocol	Défini comme " application/pkcs7-signature ". Bien que le projet de norme EDI-INT définisse aussi d'autres protocoles qui peuvent être utilisés, il est obligatoire d'utiliser le protocole " application/pkcs7-signature " pour les communications avec l'ADRC.
	Micalg	Algorithme utilisé pour calculer la valeur MIC (Message Integrity Check/vérification de l'intégrité du message). Cette valeur doit être réglée à " **sha1 "**.
	Boundary	Délimiteur à utiliser pour distinguer les parties du corps du message.
Application/<EDI Standard>	Aucun applicable	Définit la partie du corps du message contenant l'objet ÉDI transporté. Les valeurs prévues pour <EDI Standard> sont " **edi-edifact** " ou " **edi-consent** ". La valeur " edi-edifact " doit être utilisée pour indiquer que la transaction contenue dans le corps du message est en format EDIFACT. La valeur " edi-consent " sert à indiquer que la transaction contenue dans le corps du message est en format exclusif CADEX.
Application/pkcs7-signature	Aucun applicable	Définit la partie du corps du message contenant la signature numérique de l'objet ÉDI transporté.

7.5 Le contenu du délimiteur " boundary "

Si l'on se réfère à la Figure 2, on peut avoir l'impression qu'une chaîne de caractères aléatoires est utilisée dans le délimiteur, mais ce n'est pas le cas. Plus précisément, le délimiteur " boundary " est découpé comme suit :



Dans l'exemple ci-dessus, l'identificateur unique est le long nombre entier représentant la date et l'heure. Même s'il est recommandé de suivre cette convention, une implémentation particulière pourrait nécessiter une " unicité " accrue, comprenant peut-être l'ID du poste de travail, l'ID du processus et/ou l'ID du fil.

7.6 La protection du message ÉDI

Le projet de norme EDI-INT protège les échanges ÉDI au moyen de la technique signature/enveloppe. Cette technique est appliquée comme suit :

a) Le message MIME multipartie/signé est créé conformément à la spécification RFC 1847, en indiquant le protocole approprié, l'algorithme micalg et le délimiteur " boundary ".

b) La première partie du corps du message, qui contient l'objet d'échange ÉDI et un type de contenu " Application/<EDI Standard> " est assemblée. **NOTE :** dans le cas de l'application CADEX, l'objet ÉDI est simplement une transaction qui est envoyée aujourd'hui à l'Agence des douanes et du revenu du Canada. Voir aussi, à la section 7.4, les valeurs acceptables de <EDI Standard>.

b) La signature numérique de la partie du corps du message contenant l'objet d'échange ÉDI est calculée. **Elle inclut les en-têtes MIME des parties du corps du message. ****

c) La signature numérique devient la " charge utile " de données de la deuxième partie (obligatoire) du corps du message pour le message portant le type de contenu " application/pkcs7-signature ".

d) Les deux parties précédentes (objet ÉDI et signature) forment la base de la partie supérieure du corps du message ayant le type de contenu " multipartie/signé " (défini en a), ci-dessus). En outre, cet en-tête définit un protocole du type " application /pkcs7-signature ", une définition d'algorithme MIC et une définition de

délimiteur “ boundary ”.

e) Les parties ci-dessus sont chiffrées et annexées à l’en-tête du message Internet.

** Mise en garde à l’intention des réalisateurs	Tel que défini par la spécification RFC 1848, section 2.1, Service de signature numérique, la canonicalisation d’une partie du corps du message doit être effectuée **AVANT** de signer ou de vérifier la partie du corps du message. En termes simples, cela signifie que les délimiteurs de fin de ligne doivent être représentés par une paire <CR><LF> avant que les données soient signées ou vérifiées. Cela s’applique aux en-têtes ainsi qu’au contenu des parties du corps du message. “ … L’application du service de signature numérique exige que le même délimiteur de ligne soit utilisé par l’expéditeur et le destinataire. Ce document spécifie que la séquence de deux caractères <CR><LF> doit être utilisée comme délimiteur de ligne. … ” Les réalisateurs devraient noter que, dans de nombreux langages de programmation et de système d’exploitation, la représentation interne de la fin de ligne n’est pas nécessairement <CR><LF>. Ainsi, une conversion pourrait être nécessaire avant l’application ou la vérification de la signature numérique.

La figure suivante illustre un message complet d’échange ÉDI/Internet.

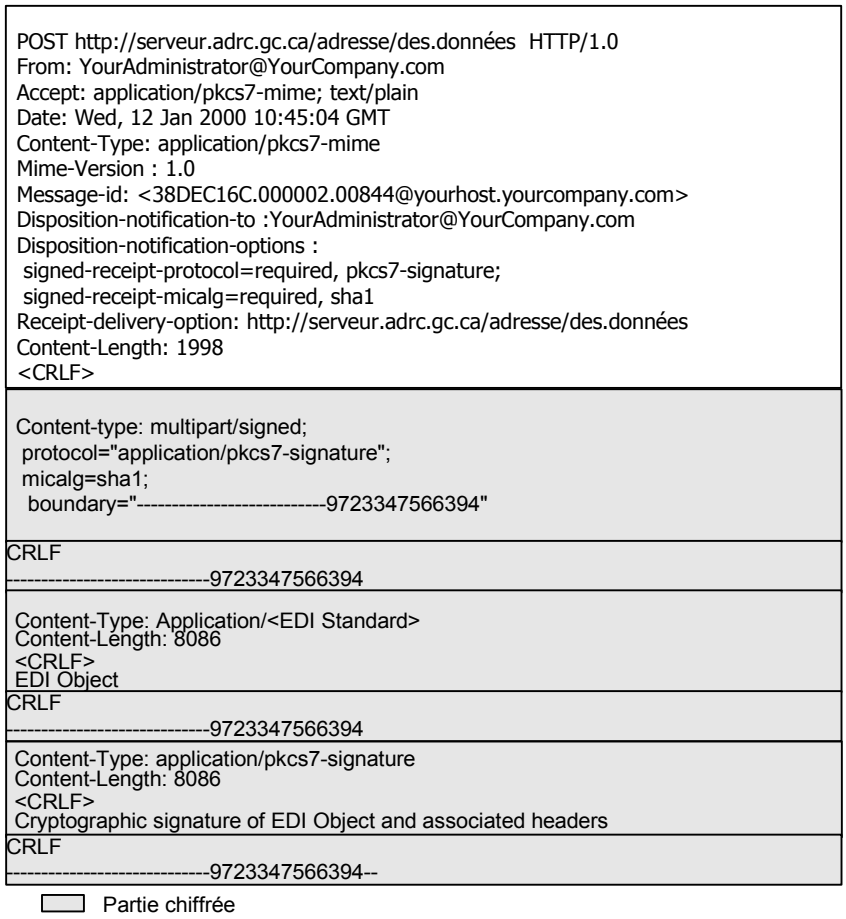


Figure 3 Le message Internet EDIINT

7.7 L'avis de livraison de message et la boucle de message sécurisée

Le projet de norme Internet " draft-ediint-as1-11.txt " élargit la spécification RFC 2298, " Message Delivery Notification (MDN) " (avis de livraison de message), en ce qu'elle s'applique à l'échange ÉDI sur l'Internet, ainsi que le concept de " boucle de transmission sécurisée ". Pour citer ce document :

> " La " boucle de transmission sécurisée " pour l'ÉDI fonctionne comme suit : une organisation envoie un message ÉDI signé et chiffré à une autre organisation, lui demandant un accusé de réception signé; par la suite, l'organisation réceptrice envoie cet accusé de réception signé à l'organisation émettrice. En d'autres termes, voici ce qui se produit :
>
> -L'organisation qui envoie les données ÉDI/EC signe et chiffre les données en utilisant PGP/MIME ou S/MIME. De plus, le message demandera qu'un accusé de réception signé soit renvoyé à l'émetteur du message.
> -L'organisation réceptrice déchiffre le message et vérifie la signature, validant ainsi l'intégrité des données et l'authenticité de l'émetteur.
>
> -L'organisation réceptrice renvoie alors un accusé de réception signé à l'organisation émettrice sous forme d'un

message d'avis de disposition du message (MDN/message disposition notification). Cet accusé de réception signé contiendra le hachage de la signature du message reçu, indiquant à l'émetteur que le message reçu a été vérifié et/ou déchiffré correctement. "

À l'évidence, la boucle de message sécurisée (ainsi que l'avis MDN) joue un rôle intégral dans le projet de norme EDIINT et le paragraphe précédent résume précisément son fonctionnement. Si précisément en fait, que ce paragraphe sert de tremplin parfait pour l'analyse de la boucle de message sécurisée.

" L'organisation qui envoie les données ÉDI/EC signe et chiffre les données en utilisant PGP/MIME ou S/MIME. "

Fait référence au message Internet basé sur S/MIME décrit dans les sections précédentes de ce document et illustré dans son intégralité à la Figure 3.

" De plus, le message demandera qu'un accusé de réception signé soit renvoyé à l'émetteur du message. "

On demande l'envoi d'un accusé de réception signé en incluant les trois en-têtes de demande suivants dans l'en-tête du message HTTP :

Disposition-notification-to: <YourAdministrator@YourCompany.com>
Disposition-notification-options :
signed-receipt-protocol=required, pkcs7-signature;
signed-receipt-micalg=required, sha1
Receipt-delivery-option: http://serveur.adrc.gc.ca/adresse/des.données

Le document " draft-ietf-ediint-as1-11.txt " définit de façon plus détaillée ces en-têtes et les options qui y sont associées.

" L'organisation réceptrice déchiffre le message et vérifie la signature, validant ainsi l'intégrité des données et l'authenticité de l'émetteur. "

Plus spécifiquement :

1) Le récepteur déchiffre le corps du message, révélant un message MIME multipartie/signé dont le corps contient deux parties.
2) Le récepteur authentifie la signature contenue dans la deuxième partie du corps du message :
    - en déchiffrant la valeur MIC envoyée à l'aide de la clé publique de l'émetteur;
    - en calculant la valeur MIC sur la première partie du corps du message conformément à la spécification RFC 1767;
    - en comparant l'égalité des deux valeurs MIC.

Si elles sont égales, la signature a été vérifiée.

L'organisation réceptrice renvoie alors un accusé de réception signé à l'organisation émettrice sous forme d'un message d'avis de disposition du message (MDN/message disposition notification). Cet accusé de réception signé contiendra le hachage de la signature du message reçu, indiquant à l'émetteur que le message reçu a été vérifié et/ou déchiffré correctement.

Plus spécifiquement :

1) le récepteur formate un avis MDN et règle le " Received-content-MIC " à la valeur MIC calculée;
2) le récepteur crée un message MIME multipartie/signé conformément à la spécification RFC 1847;
3) l'avis MDN devient la première partie du corps du message MIME multipartie/signé;
4) la deuxième partie du corps du message contient la signature numérique de la première partie, *y compris tous les en-têtes qui y sont associés.*

L'illustration suivante montre le message MIME d'avis de livraison du message.
L'emplacement des champs Received-content-MIC et Disposition présente un intérêt particulier.
Le contenu du champ Received-content-MIC est expliqué ci-dessus.
Un champ Disposition contenant " **automatic-action/MDN-sent-automatically; processed** " indique que le processus MDN était une action automatique, que l'utilisateur n'a pas donné de permission explicite pour que l'avis MDN soit généré, que l'avis MDN a été envoyé automatiquement et que le message dont il est question a été traité avec succès.
Des échecs peuvent survenir à n'importe quelle étape du traitement de la réception des messages. Ces événements entraîneront l'émission des dispositions suivantes :

Événement	Disposition
Erreurs de traitement du contenu	Automatic-action/MDN-sent-automatically; processed/ Error: decryption-failed Automatic-action/MDN-sent-automatically; processed/Error: authentication-failed Automatic-action/MDN-sent-automatically; processed/Error: integrity-check-failed Automatic-action/MDN-sent-automatically; processed /Error: unexpected-processing-error

On trouvera, à la page suivante, un exemple d'avis MDN :

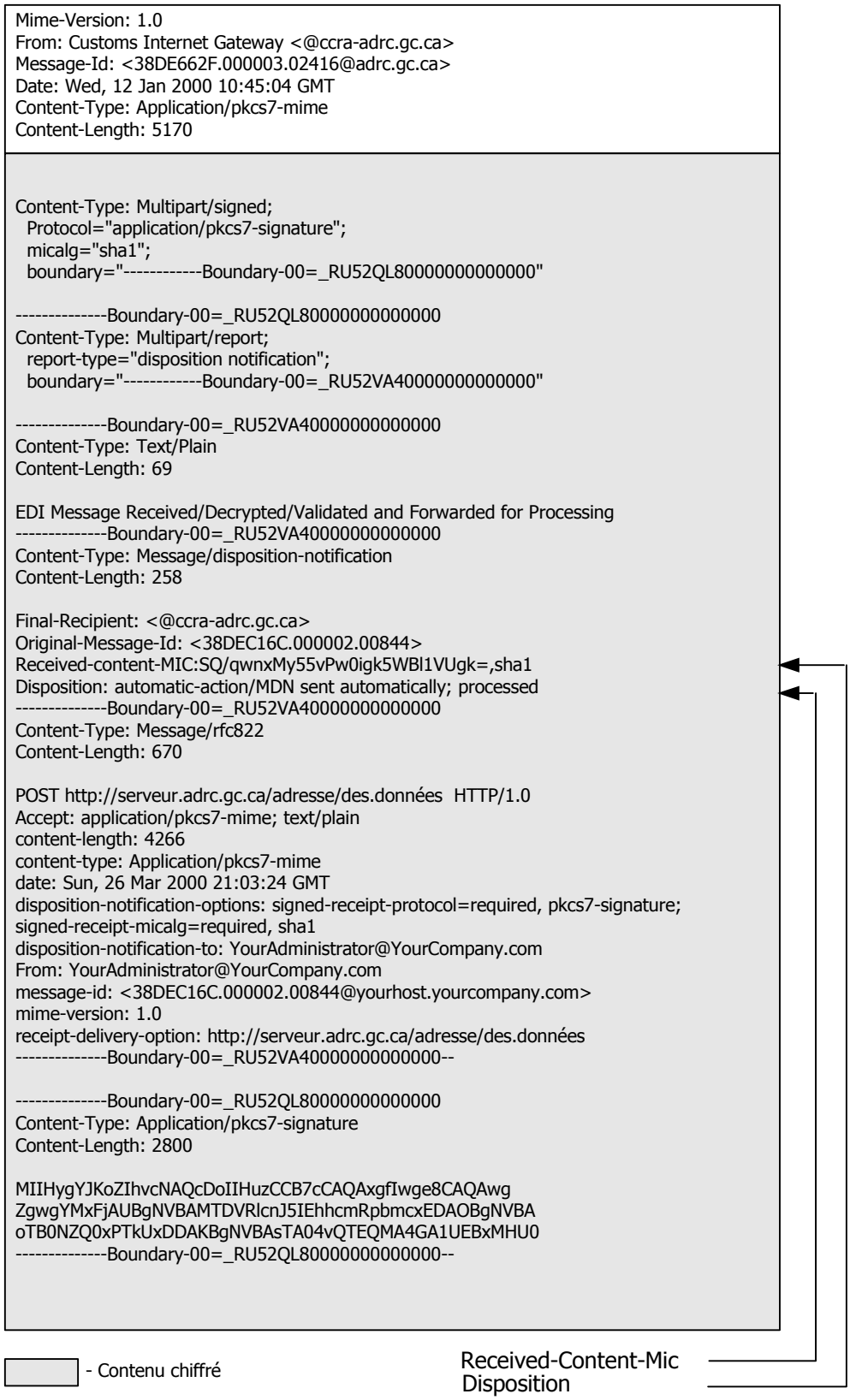

Mime-Version: 1.0
From: Customs Internet Gateway <@ccra-adrc.gc.ca>
Message-Id: <38DE662F.000003.02416@adrc.gc.ca>
Date: Wed, 12 Jan 2000 10:45:04 GMT
Content-Type: Application/pkcs7-mime
Content-Length: 5170
Content-Type: Multipart/signed;
Protocol="application/pkcs7-signature";
micalg="sha1";
boundary="----------Boundary-00=_RU52QL80000000000000"
----------Boundary-00=_RU52QL80000000000000
Content-Type: Multipart/report;
report-type="disposition notification";
boundary="----------Boundary-00=_RU52VA40000000000000"
----------Boundary-00=_RU52VA40000000000000
Content-Type: Text/Plain
Content-Length: 69
EDI Message Received/Decrypted/Validated and Forwarded for Processing
----------Boundary-00=_RU52VA40000000000000
Content-Type: Message/disposition-notification
Content-Length: 258
Final-Recipient: <@ccra-adrc.gc.ca>
Original-Message-Id: <38DEC16C.000002.00844>
Received-content-MIC:SQ/qwnxMy55vPw0igk5WBl1VUgk=,sha1
Disposition: automatic-action/MDN sent automatically; processed
----------Boundary-00=_RU52VA40000000000000
Content-Type: Message/rfc822
Content-Length: 670
POST http://serveur.adrc.gc.ca/adresse/des.données HTTP/1.0
Accept: application/pkcs7-mime; text/plain
content-length: 4266
content-type: Application/pkcs7-mime
date: Sun, 26 Mar 2000 21:03:24 GMT
disposition-notification-options: signed-receipt-protocol=required, pkcs7-signature;
signed-receipt-micalg=required, sha1
disposition-notification-to: YourAdministrator@YourCompany.com
From: YourAdministrator@YourCompany.com
message-id: <38DEC16C.000002.00844@yourhost.yourcompany.com>
mime-version: 1.0
receipt-delivery-option: http://serveur.adrc.gc.ca/adresse/des.données
----------Boundary-00=_RU52VA40000000000000--
----------Boundary-00=_RU52QL80000000000000
Content-Type: Application/pkcs7-signature
Content-Length: 2800
MIIHygYJKoZIhvcNAQcDoIIHuzCCB7cCAQAxgfIwge8CAQAwg
ZgwgYMxFjAUBgNVBAMTDVRlcnJ5IEhhcmRpbmcxEDAOBgNVBA
oTB0NZQ0xPTkUxDDAKBgNVBAsTA04vQTEQMA4GA1UEBxMHU0
----------Boundary-00=_RU52QL80000000000000--
- Contenu chiffré
Received-Content-Mic
Disposition

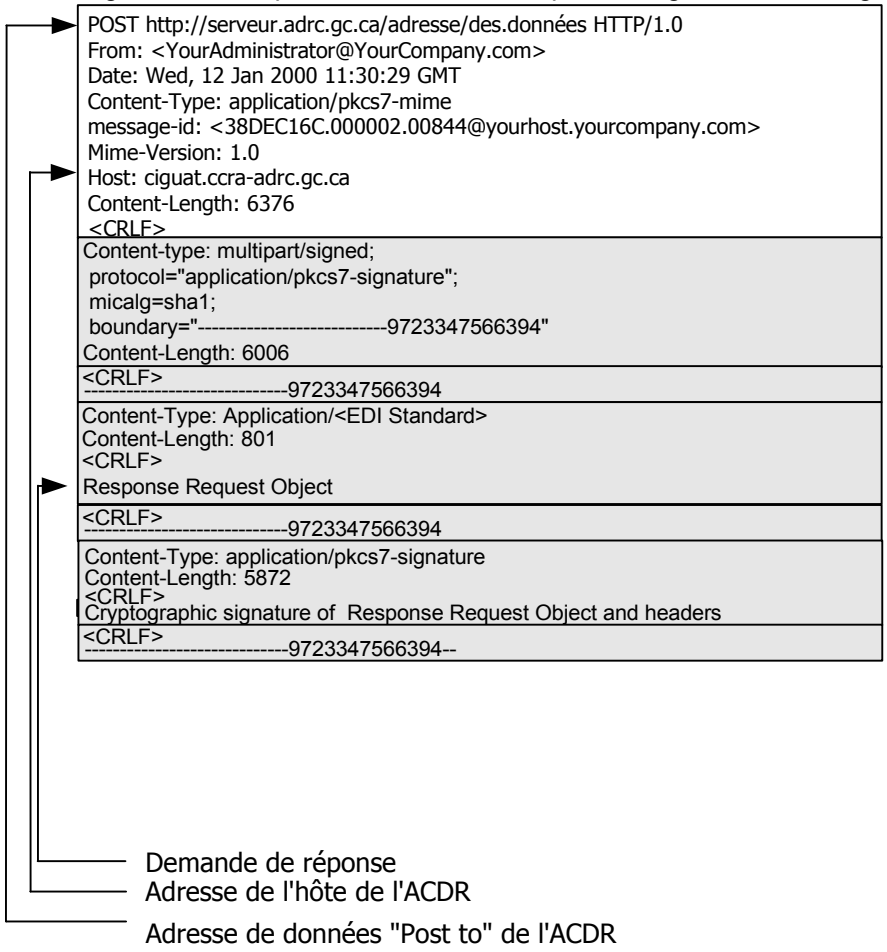
Figure 4 Le message d'avis de livraison de message (MDN)

On trouvera des renseignements supplémentaires sur les erreurs et/ou les avertissements d'erreurs de traitement du contenu de l'objet ÉDI indiqués dans le champ Disposition dans les documents " MIME-based Secure EDI " et " An Extensible Message Format for Message Disposition Notification " ainsi que dans le document " draft-ietf-ediint-as1-11.txt ", section 5.3.

Un avis MDN sera émis pour chaque message ÉDI qui sera envoyé pour traitement à l'ADRC. L'Agence demandera aussi l'envoi d'avis MDN lorsqu'elle enverra des transactions ÉDI à ses partenaires commerciaux. Les partenaires commerciaux devraient utiliser le même format général pour le renvoi des avis MDN à l'ADRC. À noter que, conformément à la spécification (RFC 2298, Section 2.1), les avis MDN ***ne font pas*** l'objet d'un accusé de réception avec avis MDN.

7.8 La demande de téléchargement de réponses de transactions

Pour recevoir les réponses de transactions qui pourraient être en file d'attente dans l'ordinateur hôte, il faut envoyer un message Internet particulier en indiquant l'adresse de données du service responsable du téléchargement des réponses. Voici un exemple de ce genre de message :



À noter que ce message est simplement une variante du message " Content-Type: Application/pkcs7-mime " utilisé pour la soumission de l'objet ÉDI. Voici en quoi ce message diffère d'un message de soumission d'objet ÉDI :

Adresse de données	L'adresse URI de la ressource chargée de traiter la demande de réponse différera de celle de la ressource chargée de traiter les soumissions d'objets ÉDI.

Demande de réponse	L'objet Demande de réponse *peut* être toute transaction valide formatée pour Edifact ou Cadex (note : la transaction ne sera toutefois pas traitée comme une transaction ÉDI. Elle sert simplement à demander un téléchargement).

Par suite de la soumission ci-dessus, le service de téléchargement de transactions de l'ADRC, appelé CigWasGet0 et situé dans CigWasOp/CigWas :

a) validera l'identité de l'émetteur de la demande;
b) et, si la validation réussit, enverra au demandeur toutes les transactions destinées au courtier du client demandeur.

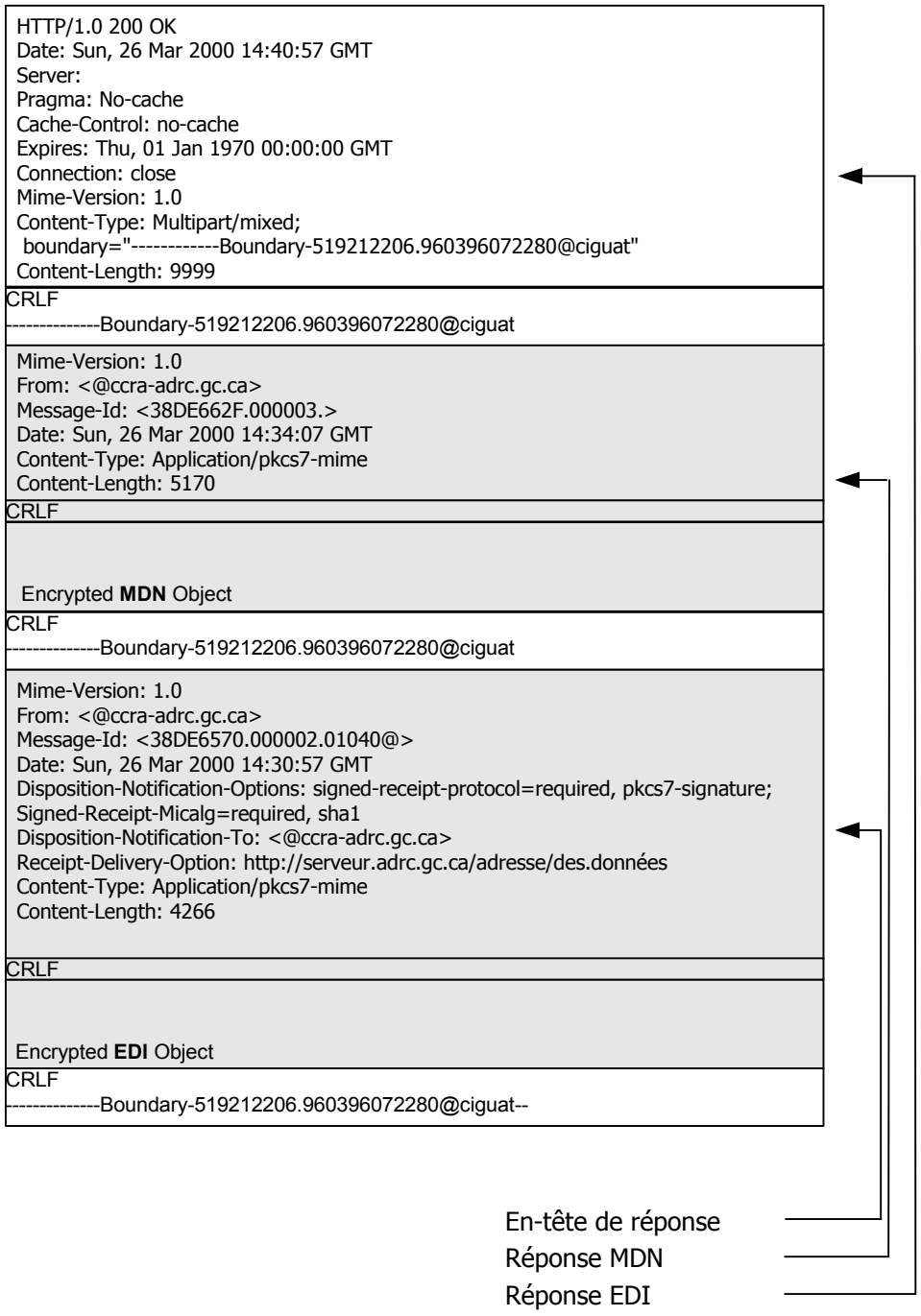
Veuillez également noter qu'une transaction de " demande de téléchargement " ***ne doit pas*** contenir de demande de réponse MDN, c.-à-d. que les en-têtes Disposition-Notification-To:, Disposition-Notification-Options: et Receipt-Delivery-Options: sont omis

7.9 Le message de réponse

Une fois que le partenaire commercial a demandé un téléchargement en utilisant la technique décrite ci-dessus, toutes les transactions ÉDI et MDN en attente de livraison seront préparées et formatées pour transmission au partenaire commercial.

Un format multipartie est utilisé pour que les transactions individuelles puissent être distinguées les unes des autres.

Voici un exemple de message de réponse type :



Les zones ombrées correspondent aux transactions ÉDI et MDN.

Nom du champ de l'en-tête de réponse	Sous-champs	Description	Référence
HTTP Response[7]	HTTP Version	Actuellement réglé à " HTTP/1.0 ".	RFC1945, section 3.1
	Status Code	Voir la section 7.10 du présent document.	RFC1945, section 9
	Reason Phrase	Voir la section 7.10 du présent document.	RFC1945, section 9
Date	Aucun	La date/heure à laquelle le message a été envoyé.	RFC1945, section 10.6
Server	Aucun	Contient de l'information sur le logiciel utilisé par le serveur d'origine pour traiter la demande.	RFC1945, section 10.14
Pragma	Aucun	Sert à indiquer aux serveurs " proxy " intermédiaires que la réponse ne devrait pas être mise en cache.	RFC1945, section 10.12
Cache-Control	Aucun	Sert à indiquer aux serveurs " proxy " intermédiaires que la réponse ne devrait pas être mise en cache. *Ce champ est inclus à des fins de conformité.*	RFC2616, section 14.9.1
Expires	Aucun	Sert à indiquer aux serveurs " proxy " intermédiaires que la réponse ne devrait pas être mise en cache.	RFC1945, section 10.7
Connection	Aucun	Permet à l'émetteur de demander des options qui s'appliqueront à la connexion particulière. Actuellement réglé à " close ".	
Mime-Version	Aucun	Actuellement réglé à " 1.0 ".	
Content-Type		Sert à spécifier le type de support du corps de message envoyé au destinataire. Est réglé à " multipart/mixed ".	Draft-ietf-ediint-as2-06
Boundary	Aucun	Délimiteur à utiliser pour séparer les parties du corps du message.	RFC1521
Content-Length	Aucun	Spécifie la longueur de l'ensemble du corps du message en décimale.	RFC1945, section 10.4
MDN Response Fields		Voir la section 7.1 du présent document.	
EDI Response Fields		Voir la section 7.1 du présent document.	

7.10 Les codes de réponse

La spécification HTTP 1.0 (RFC1945) définit les codes d'état qui peuvent être livrés à un client en réponse à une demande. En général, ces codes se répartissent dans les catégories suivantes :

1xx - codes d'information
2xx - codes de succès
3xx - codes de redirection (réacheminement)
4xx - codes d'erreur client
5xx - codes d'erreur serveur

[7] dont les sous-champs sont délimités par un espace (0x20).

La section suivante résume les codes de réponse HTTP que le client peut s'attendre à recevoir du serveur de l'ADRC et leurs significations en ce qu'elles s'appliquent à la mise en œuvre actuelle du serveur[8]. À noter que ces significations peuvent être modifiées et/ou étendues dans les futures implémentations.

Code d'état	Signification
200	**OK** ; la demande a réussi. Dans le contexte de l'envoi d'une transaction, ce code indique que la transaction a été reçue, validée avec succès et mise en file d'attente pour exécution. Dans le contexte de la réception d'une transaction, ce code indique que la demande de l'utilisateur a été reçue, validée avec succès et renvoyée avec les réponses qui ont été mises en file d'attente sur l'ordinateur hôte.
204	**No Content (pas de contenu)**; en réponse à une demande de téléchargement, ce code indique que la demande a été reçue et traitée avec succès, mais qu'aucune réponse ne sera envoyée pour l'instant.
301	**Moved Permanently (déplacé de façon permanente)**; ce code indique que la ressource a été déplacée de façon permanente à un nouvel endroit et que les références futures devraient utiliser dans les demandes une nouvelle adresse URI (adresse de données de l'ADRC). Contacter l'Agence des douanes et du revenu du Canada pour obtenir la nouvelle adresse.
400	**Bad Request (demande incorrecte)**; ce code indique que la syntaxe de la demande envoyée par le client était incorrecte. De plus, il a été impossible d'obtenir de l'information précise au sujet de l'erreur.
403	**Forbidden (interdit)**; ce code indique que le serveur a compris la demande mais refusé d'y répondre. Cela indique que le profil d'environnement du client n'incluait pas l'accès à la ressource demandée.
404	**Not Found (introuvable)**; ce code indique que : 1. la ressource demandée n'est pas disponible, 2. l'adresse de données fournie était mal formée ou inconnue.
500	Le serveur HTTP n'est pas disponible.
503	**Service Unavailable (service non**

[8] En d'autres termes, tandis que ces codes ont un sens générique dans le cadre de la spécification, cette section décrit, en plus de ce sens générique, leur signification dans le cadre de l'implémentation des serveurs de RC.

disponible); ce code indique que le serveur HTTP ou l'un de ses composants est *temporairement* incapable de traiter la demande.

Tous les autres codes de retour devraient être interprétés comme des erreurs à moins d'indication contraire dans les publications et/ou bulletins subséquents de l'ADRC.

Mise à garde à l'intention des réalisateurs	Dans cette dernière section, de nombreuses données sont présentées de façon apparemment statique. Soulignons que ce ***n'est pas*** le cas. Les en-têtes HTTP et leur contenu pourraient changer avec le temps par suite de changements système ou pour améliorer l'efficience. Par conséquent, il est recommandé au lecteur d'implémenter les zones de données précédentes de manière à ce qu'elles puissent être dynamiquement modifiées (c.-à-d. sans recompiler le programme).

Voici un exemple d'une réponse " no data queued " (no content/pas de contenu, code 204) du serveur :

```
HTTP/1.0 204 ok
Date: Mon, 05 Jun 2000 19:04:40 GMT
Server:
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Connection: close
Content-Type: text/plain
```

8. La cryptographie - Aperçu

Pour protéger un message, l'émetteur transforme ce message (en texte clair) en une forme, appelée cryptogramme, qui n'est pas reconnaissable par les humains. Ce processus est appelé *chiffrement* ou *cryptographie*. Le cryptogramme est ensuite transmis au récepteur par un moyen quelconque. Sur réception du message, le destinataire convertit le cryptogramme en son format original. C'est ce qu'on appelle le déchiffrement (ou décryptage, décodage).

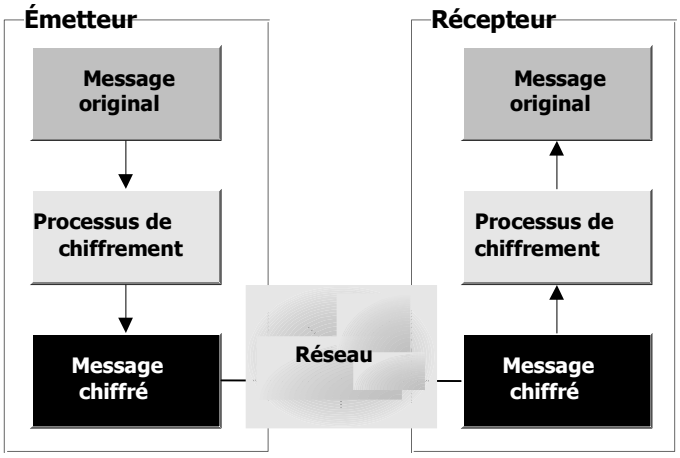


Figure 5 - Le processus de chiffrement/déchiffrement

Si le message est intercepté, l'intrus n'a accès qu'au cryptogramme inintelligible. Un bon système de cryptographie rend difficile pour l'intrus de recalculer le texte en clair original, même s'il connaît le processus utilisé pour chiffrer ce texte.

Avant d'envoyer un message chiffré, l'émetteur doit posséder deux éléments d'information pour lesquels il doit avoir l'accord du récepteur :

- La méthode (ou algorithme) qui sera utilisée pour convertir le texte original en cryptogramme.
- La valeur mathématique (ou clé) qui sera utilisée pour faire la transformation.

Une fois cela convenu, l'émetteur peut chiffrer le message. Le destinataire reçoit le cryptogramme, le déchiffre et interprète le message normalement.

8.1 La cryptographie à clé unique

La forme la plus ancienne de la cryptographie utilisait une clé unique pour chiffrer le cryptogramme et pour déchiffrer le texte en clair original. Cette méthode de chiffrement est appelée cryptographie symétrique. Le problème posé par cette forme de cryptographie est qu'il est absolument essentiel que la clé demeure secrète. Si des tiers viennent à connaître la clé, alors le message n'est pas fiable. Les parties doivent donc s'entendre sur une nouvelle clé, mais il faut également que l'échange de cette information se fasse en privé.

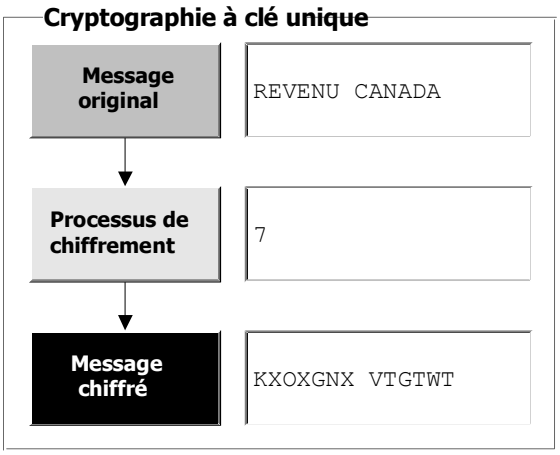


Figure 6 - Cryptographie à clé unique

Considérons le diagramme présenté à la Figure 5 dans l'exemple suivant. Il faut qu'un message soit transmis sur un réseau non protégé, ou public, comme l'Internet. Pour faire en sorte qu'il soit plus difficile pour un intrus de décoder le contenu de ce message, l'émetteur et le récepteur décident d'ajouter une valeur aléatoire à chaque octet du message. Le cryptogramme ainsi obtenu est complètement différent du message original, la clé est aléatoire (ce pourrait être n'importe quel nombre), et on peut inverser le processus pour décoder le message original (en soustrayant simplement la clé). L'inconvénient, dans cet exemple, est que si l'intrus connaît l'algorithme utilisé, il lui suffirait alors de faire passer le cryptogramme par les 10 clés possibles pour finir par arriver au message original. Les algorithmes utilisés par Entrust sont beaucoup plus robustes et utilisent des clés beaucoup plus longues (actuellement, ces clés peuvent atteindre 2 048 bits). Si un intrus voulait décoder une clé d'une longueur de 2 048 bits et avait accès à un ordinateur capable de vérifier 1 million de clés possibles en une seconde, il lui faudrait quand même 1 0248•10^{604} années pour vérifier toutes les clés possibles. Si l'on disposait d'un milliard d'ordinateurs capables de vérifier un milliard de clés à la seconde, il faudrait quand même 1 0248•10^{592} années.

8.2 La cryptographie à clé publique

La cryptographie à clé publique, aussi appelée cryptographie asymétrique, consiste à utiliser une paire de clés pour transmettre de l'information. Chaque utilisateur a deux clés, une clé publique et une clé privée. La clé publique est mise à la disposition directe de toute personne qui désire envoyer de l'information chiffrée à l'utilisateur, qui se servira de sa clé privée pour déchiffrer le message. Dans ce processus, l'émetteur a l'assurance que seule la personne qui possède la bonne clé privée peut déchiffrer le message, car toute autre clé ne produira que du texte illisible.

8.3 Les signatures numériques

Une signature numérique est un moyen électronique de valider l'intégrité d'un élément de données. Par exemple, supposons qu'une personne reçoit un document électronique. Comment le récepteur peut-il savoir si le fichier a été trafiqué par un tiers? Même si le message est chiffré, le récepteur doit s'assurer que le fichier n'a pas été modifié par un moyen ou un autre. Cela est particulièrement important pour les applications de commerce électronique.

On résout le problème de l'intégrité des données en créant une signature électronique des données. C'est ce qu'on appelle souvent un hachage du texte en clair original. Une fonction de hachage prend des données d'entrée de n'importe quelle longueur et produit un hachage d'une longueur finie, habituellement de 128 ou 160 bits. Ce hachage peut représenter l'ensemble des données s'il possède les propriétés suivantes :

- *Cohérence*
  Les mêmes fichiers d'entrée produiront toujours les mêmes sorties (c.-à-d. hachage).
- *Imprévisibilité*
  Étant donné un hachage particulier, il sera pratiquement impossible d'inverser le processus de hachage et de produire le message original.
- *Volatilité*
  Cela peut sembler contradictoire par rapport à la première propriété, mais il est essentiel qu'un léger changement dans le message d'entrée produise un changement radical dans le hachage. Cela réduit la possibilité qu'un changement apporté à un bit de données soit ignoré par la fonction de hachage et produise le même hachage.

Le tableau suivant présente un exemple de hachage. À noter que les messages originaux sont a) très différents par suite du hachage et b) qu'une modification même mineure du message d'entrée produit un hachage très différent. Ces hachages ont été générés à l'aide du *Secure Hash Algorithm*

(l'algorithme de hachage sécurisé standard de l'industrie informatique), défini par l'organisme américain NIST (National Institute of Standards and Technology) :

Message	**Hachage du message** (utilisant base16 pour représenter les bits)
Today is February 01, 1998	ADE4F5EE 81BCC565 6F225414 CA9615DD $E09D1754_{16}$
Today is February 02, 1998	F6181A1E BBBCD329 60B9CF9A 138649A3 $5E4F138C_{16}$

8.4 La mise en œuvre d'Entrust

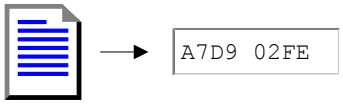
La solution d'ICP Entrust utilise tous les processus décrits ci-dessus pour protéger les communications de données. Plusieurs composants d'infrastructure sont nécessaires au bon fonctionnement d'une infrastructure à clé publique. D'abord, chaque utilisateur a besoin d'un moyen pour partager ses clés publiques avec le public. À l'Agence des douanes et du revenu du Canada, une autorité de certification et un répertoire sont disponibles à cette fin. Chaque utilisateur a quatre clés :

- Une clé de chiffrement privée et une clé de chiffrement publique
- Une clé de signature privée et une clé de signature publique

Les illustrations suivantes expliquent comment Entrust utilise ces clés pour protéger les données électroniques. Ces diagrammes supposent que l'émetteur et le récepteur ont mutuellement accès à leurs clés publiques et qu'ils se fient à la source qui leur a fourni ces clés.

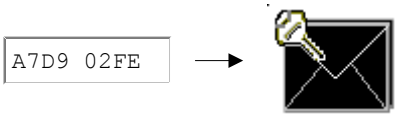
1. *Signer les données*

   La première partie du processus consiste à créer un hachage des données à transmettre. C'est également ce qu'on appelle la vérification de l'intégrité du message ou MIC (Message Integrity Check). En utilisant l'algorithme de hachage approprié, on crée un identificateur unique qui sera utilisé (dans les faits) pour signer le message. (Note : la convention adoptée pour représenter un hachage est d'utiliser le format hexadécimal).



2. *Chiffrer le hachage*

   Maintenant, l'information qui sera utilisée pour valider les données originales doit être protégée avant d'être transmise. Pour ce faire, l'émetteur utilisera sa clé de signature privée pour chiffrer le hachage.



3. *Chiffrer les données*

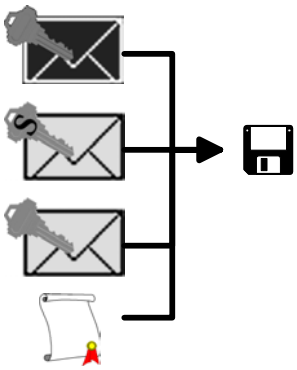
   Les données peuvent maintenant être chiffrées. Pour ce faire, le système Entrust créera une nouvelle clé symétrique unique et ponctuelle avec laquelle il chiffrera les données originales. Un processus de chiffrement symétrique est utilisé car cette méthode est généralement beaucoup plus rapide qu'un algorithme asymétrique.

4. *Chiffrement de la clé unique*

   Maintenant que les données sont protégées, il faut envoyer la clé unique au récepteur pour qu'il puisse déchiffrer le message. Pour cela, l'émetteur localisera la clé de chiffrement publique du récepteur et s'en servira pour chiffrer la clé.

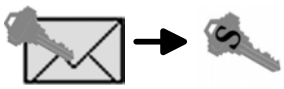
5. *Livrer l'information chiffrée*

Le dernier élément à inclure est l'information relative au certificat public de l'émetteur. Ce certificat indiquera au récepteur où trouver l'information publique de l'émetteur. Ensuite, les données sont transmises au récepteur, au moyen de la méthode désirée. Il existe plusieurs méthodes, notamment : disquette, courrier électronique, FTP, HTTP, etc. À noter que toute cette information est contenue dans un seul fichier, et non trois, comme le diagramme pourrait le suggérer. Si le fichier original est appelé Document.doc, alors le fichier chiffré serait nommé `Document.ent`. Un des avantages de la technologie Entrust est qu'elle peut comprimer les données chiffrées, ce qui a généralement pour résultat que l'information chiffrée est moins volumineuse que le format original. Cela réduit le temps de transfert et la largeur de bande nécessaire.



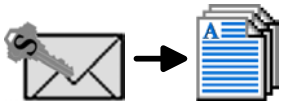
6. *Déchiffrer la clé unique*

Maintenant, le récepteur doit déchiffrer le message. La première tâche est de déterminer la clé unique utilisée par l'émetteur pour chiffrer les données. Pour ce faire, le récepteur utilisera sa propre clé privée.



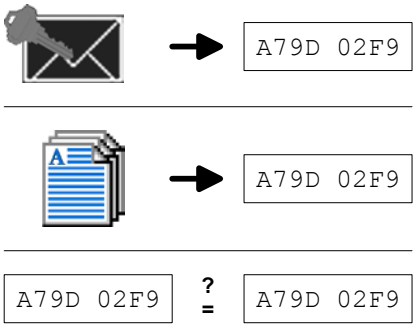
7. *Déchiffrer les données*

À l'aide de cette clé symétrique, le récepteur déchiffrera les données. Elles sont maintenant lisibles, mais le récepteur n'est pas tout à fait certain que les données sont fiables.



8. *Valider les données*

Pour vérifier l'identité de l'émetteur des données et valider les données elles-mêmes, le récepteur commencera par localiser la clé de signature publique de l'émetteur, puis déchiffrera la valeur de hachage qui a été transmise. Le récepteur calculera ensuite le hachage des données originales. Si les deux valeurs de hachage sont identiques, le récepteur est alors assuré de l'identité de l'émetteur et du fait que les données n'ont pas été altérées.



9. Les mots de passe

Il faut un mot de passe pour accéder au contenu du profil Entrust. Ce profil permet alors d'accéder à de l'information de nature délicate comme les clés de chiffrement et de signature. Il est donc essentiel que le mot de passe demeure secret.

Il est recommandé que l'accès au mot de passe de l'utilisateur soit restreint.

Une fois qu'un mot de passe a été utilisé dans un code de programme (c.-à-d. EntrustProfile.logon()), il est recommandé que la zone de données contenant le mot de passe soit écrasée avant la désallocation ou la perte de portée (dans le cas du langage C++) et/ou la " collecte des ordures " (dans le cas de Java).

Il ***n'est pas*** recommandé d'utiliser ces spécifications pour créer une application récupérable " sans intervention humaine ". En d'autres termes, un opérateur humain doit être présent pour entrer le mot de passe nécessaire au démarrage de l'application.

Notes.

Annexe B – Acquisition du logiciel

Acquisition du logiciel

Introduction

Pour participer au Projet de passerelle Internet des douanes (PID) de l'ADRC et vous y inscrire, vous devez acheter un certificat délivré par l'autorité de certification de l'ADRC.

Pour recevoir votre certificat de l'AC de l'ADRC, vous devez d'abord acheter le droit d'utiliser ce certificat et le logiciel cryptographique client qui vous permettent de récupérer ce certificat au moyen d'un processus de génération de clé.

L'ADRC utilise la version 5.0 Entrust Authority® et les clients doivent utiliser Entrust Entelligence® version 5.0 ou une version Entrust 100 % compatible conforme aux spécifications énoncées à l'annexe A.

Préalables techniques

Logiciel

Un des systèmes d'exploitation suivant doit tourner sur le système où sera installé le logiciel client Entrust Entelligence® version 5.0 :

Microsoft®Windows®95 (avec Service Pack 1 ou supérieure)
Microsoft®Windows®98
Microsoft®Windows®NT 4.0 (Service Pack 4 ou supérieure)
Microsoft®Windows®2000
MacIntosh Power PC, système 7.1 ou supérieure

Matériel

Voici la configuration minimale des postes de travail sur lesquels doit tourner le logiciel client version 5.0 Entrust Entelligence ® :

Ordinateur personnel de type Pentium
32 Mo de mémoire RAM
Au moins 12 Mo d'espace disque
Un lecteur de CDROM
Le mécanisme de transport TCP/IP

Acquisition

Veuillez communiquer avec le fabricant ou avec un détaillant autorisé pour connaître les modalités et le prix d'achat du logiciel client. N'oubliez pas de mentionner que vous participez au Projet de passerelle Internet des douanes de l'ADRC.

Annexe C – Exigences techniques ICP/ Internet

Exigences techniques ICP/ Internet

Station de travail

Logiciel

Le navigateur Web chargé sur la station de travail doit supporter un logiciel de chiffrement de 128 bits, notamment :

Microsoft®Internet Explorer 4.0, ou supérieure
Netscape®Communicator 4.5, ou supérieure

Connexion Internet

L'autorité d'inscription, le répertoire public et l'autorité de certification automatisés de l'ADRC ne sont accessibles que sur Internet. D'où la nécessité d'être connecté à Internet. Il peut s'agir d'une connexion sur demande fournie par un fournisseur de services Internet (FSI) ou une infrastructure de réseau local. Le participant doit communiquer les détails techniques aux entités locales de technologie de l'information ou au FSI pour s'assurer que la connexion est adéquate.

Coupe-feu

Les règles de configuration du coupe-feu suivantes doivent être communiquées aux ressources techniques locales et appliquées au coupe-feu local, les communications avec l'ICP de l'ADRC ne pouvant se faire sans la mise en application de ces règles.

Port 389 – LDAP

La version 3 du Lightweight Directory Access Protocol (LDAP) est un protocole d'extraction de données universel que les programmeurs peuvent utiliser comme interface courante pour extraire des données de diverses sources, notamment de répertoires et des bases de données. L'ICP de l'ADRC utilise un répertoire X500 comme entrepôt public des certificats et des listes de révocation des certificats (LRC). Le logiciel client Entrust consulte cet entrepôt pour extraire les tout derniers certificats et les listes de révocation de certificat courantes pour s'assurer que la relation de confiance établie est toujours valide. Le répertoire est consulté chaque fois qu'un client se connecte.

Règle de coupe-feu : Ne permettre que les connexions TCP vers 207.245.213.12.

Port 709 – Entrust KMS

Le protocole Entrust Key Management Service (KMS) est utilisé par l'autorité de certification (AC) pour communiquer avec les clients. Après la création initiale de leur profil, les clients doivent rarement communiquer avec l'AC sauf s'ils doivent modifier leur profil en cas de problème. Par exemple, s'ils doivent récupérer leur profil parce qu'il a été altéré, parce qu'ils ont oublié le mot de passe, parce que les certificats sont expirés et parce que les clés doivent être mises à jour.

Règle de coupe-feu : Ne permettre que les connexions TCP vers 207.245.213.141.

Port 829 – PKIX-CMP

PKIX est un ensemble de normes qui assure l'interopérabilité entre les différentes produits de l'ICP. La version 5 de Entrust supporte ce protocole auquel passeront, nous l'espérons, tous les clients de l'ADRC. Si tous les clients utilisent chez vous la version 5, appliquez la règle ci-dessous et supprimez la règle en rapport avec le port 709.

Règle de coupe-feu : Ne permettre que les connexions TCP vers 207.245.213.141.

Évaluation du risque

L'ouverture de n'importe quel port d'un coupe-feu représente un certain risque car un nombre supplémentaire de ports peuvent faire l'objet d'une attaque potentielle, principalement du type « déni de service ». Aucun point faible particulier n'a été identifié en rapport avec les ports mentionnés précédemment. La configuration adéquate des règles de coupe-feu, conformément aux recommandations précédentes, limite le risque, car seules les demandes de connexion vers l'extérieur sont autorisées (les demandes de connexion aux ports en provenance d'Internet seront refusées).

Lorsqu'une demande de connexion vers l'extérieur interne autorisée par un port sélectionné est accordée, la connexion vers l'intérieur de retour n'est autorisée que si la source correspond à la destination cible spécifiée dans le message original vers l'extérieur.

Points de recherche cible

Tel que l'opération de choisir un destinataire dans un courriel afin que celui ci parvienne à la destination prévue, l'usager doit spécifier quel est le certificat cible à utiliser dans le processus de chiffrement et de signature digitale afin que le message demeure en sécurité spécifiquement pour le destinataire choisi.

La Passerelle Internet des Douanes utilise deux certificats cible, le premier pour permettre la vérification en mode Ops et le deuxième pour soumettre les transactions en mode production. Respectivement, ces certificats sont:

Vérification en mode Ops;

cn=Ops CCRA-ADRC GW+serialNumber=100063,ou=EQUIP,ou=EXTERN,ou=CCRA-ADRC,o=GC,c=CA

Transaction en mode production;

cn=Prod CCRA-ADRC GW+serialNumber=100062,ou=EQUIP,ou=EXTERN,ou=CCRA-ADRC,o=GC,c=CA