Groupe de travail Réseau
Request for Comments : 3335
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

T. Harding, Cyclone Commerce
R. Drummond, Drummond Group
C. Shih, Gartner Group
septembre 2002

Échange de données d'affaire sécurisées d'homologue à homologue fondé sur MIME sur l'Internet

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit comment échanger de façon sûre des données d'affaire structurées en utilisant le transport SMTP pour les échanges de données électroniques (EDI, *Electronic Data Interchange*) (EDI – soit le comité américain de normalisation X12 soit UN/EDIFACT, *Electronic Data Interchange for Administration, Commerce and Transport)*, XML ou d'autres données utilisées pour les échanges de données d'affaires. Les données sont formatées en utilisant les types de contenu MIME standard. L'authentification et la protection de la confidentialité sont obtenues à l'aide de la syntaxe de message cryptographique (S/MIME, *Cryptographic Message Syntax*) ou les parties de corps de sécurité OpenPGP. L'authentification des accusés de réception fait usage de réponses multipartie/signées au message SMTP original.

Table des Matières

1. Introduction....2
2. Généralités....2
2.1 Objet de lignes directrices de sécurité pour les EDI MIME....2
2.2 Définitions....2
2.3 Hypothèses....3
3. RFC référencées et leur apport....5
3.1 SMTP [RFC2821]....5
3.2 Format de message de texte [RFC0822]....5
3.3 Multiparties de sécurité pour MIME [RFC1847]....5
3.4 Multipartie/rapport [RFC1892]....5
3.5 Contenu d'EDI [RFC1767]....5
3.6 PGP/MIME [RFC2015], [RFC3156], [RFC2440]....5
3.7 MIME [RFC2045], [RFC2046], et [RFC2049]....5
3.8 Notification de disposition de message[RFC2298]....5
3.9 Spécifications de message S/MIME version 3 [RFC2633] et [RFC2630]....5
4. Structure d'un message MIME EDI - Applicabilité....5
4.1 Introduction....5
4.2 Structure d'un message EDI MIME - PGP/MIME....6
4.3 Structure d'un message EDI MIME - S/MIME....6
5. Récépissés....7
5.1 Introduction....7
5.2 Demande d'un récépissé signé....8
5.3 Format de notification de disposition de message....9
5.4 Traitement de la notification de disposition de message....12
6. Traitement du certificat de clé publique....14
6.1 Approche à court terme....14
6.2 Approche à long terme....14
7. Considérations pour la sécurité....14
8. Remerciements....15
9. Références....15
Appendice Formulaire d'enregistrement auprès de l'IANA....16

A.1 Enregistrement par l'IANA du paramètre de disposition de contenu signed-receipt-protocol.....16
A.2 Enregistrement par l'IANA du paramètre de disposition de contenu signed-receipt-micalg.....16
A.3 Enregistrement par l'IANA du nom de champ d'extension MDN Received-content-MIC.....16
Adresse des auteurs.....16
Déclaration complète de droits de reproduction.....16

1. Introduction

Des travaux précédents sur les EDI Internet se concentraient sur la spécification des types de contenu MIME pour les données d'EDI ([RFC1767]). Le présent document dépasse la RFC1767 pour spécifier l'utilisation d'un ensemble complet de caractéristiques de sécurité des données, spécifiquement la confidentialité des données, l'intégrité/authenticité des données, la non répudiation de l'origine et la non répudiation de réception. Le présent document reconnaît aussi des RFC contemporaines et tente de "réinventer" aussi peu que possible. Bien que le présent document se concentre spécifiquement sur les données d'EDI, tous les autres types de données sont aussi pris en charge.

Avec une amélioration dans le domaine des "récépissés", comme décrit ci-dessous (5.2), un EDI Internet sécurisé fondé sur MIME peut être réalisé en utilisant et se conformant aux RFC suivantes :
- RFC 821 SMTP
- RFC 822 Formats des messages de texte
- RFC 1767 Type de contenu d'EDI
- RFC 1847 Multiparties de sécurité pour MIME
- RFC 1892 Multipart/Report
- RFC 2015, 3156, 2440 MIME/PGP
- RFC 2045 à 2049 MIME
- RFC 2298 Notification de disposition de message
- RFC 2630, 2633 Spécification S/MIME v3

Notre intention est ici de définir clairement et précisément comment ces RFC sont utilisées conjointement et ce qui est exigé des agents d'utilisateur pour être conformes au présent document.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Généralités

2.1 Objet de lignes directrices de sécurité pour les EDI MIME

L'objet de ces spécifications est de s'assurer de l'interopérabilité entre les agents d'utilisateurs d'EDI, lorsque ils invoquent certaines ou toutes les caractéristiques de sécurité communément attendues. Le présent document est aussi NON limité à la stricte utilisation dans le domaine de l'EDI, mais s'applique à toute application de commerce électronique où les données d'affaire doivent être échangées sur l'Internet d'une manière sûre.

2.2 Définitions

2.2.1 Termes

EDI *(Electronic Data Interchange)* échange de données électroniques
EC *(Electronic Commerce)* commerce électronique
Réçépissé : message fonctionnel qui est envoyé d'un receveur à un envoyeur pour accuser réception d'un échange EDI/EC.
Reçu signé : comme ci-dessus mais avec une signature numérique.
MDN *(Message Disposition Notification)* Notification de disposition de message : format de messagerie Internet utilisé pour porter un reçu. Ce terme est utilisé de façon interchangeable avec reçu. Un MDN signé est un reçu signé.
NRR *(Non-repudiation of Receipt)* : non répudiation de reçu : NRR est un "événement légal" qui survient lorsque l'envoyeur original d'un échange d'EDI/EC a vérifié le reçu signé qui revient du receveur. NRR N'EST PAS un message fonctionnel ou technique.
PGP/MIME : sécurité d'enveloppe numérique fondée sur la norme Pretty Good Privacy (PGP) de (Zimmerman), intégrée avec les multiparties de sécurité MIME [RFC1847].

S/MIME : format et protocole pour ajouter les services de signature numérique et/ou de chiffrement aux messages MIME Internet.

2.2.2 Boucle de transmission sûre

Le présent document se concentre sur les formats et les protocoles pour échanger du contenu d'EDI qui a eu une sécurité appliquée en utilisant l'environnement de messagerie de l'Internet.

La "boucle de transmission sûre" pour l'EDI implique qu'une organisation envoie un échange d'EDI signé et chiffré à une autre organisation, demandant un récépissé signé, suivi ultérieurement par le renvoi par l'organisation receveuse de ce reçu signé à l'organisation envoyeuse. En d'autres termes, il se passe ceci :

- L'organisation qui envoie les données EDI/EC signe et chiffre les données en utilisant PGP/MIME ou S/MIME. De plus, le message va demander qu'un récépissé signé soit retourné à l'envoyeur du message.
- L'organisation qui reçoit déchiffre le message et vérifie la signature, ce qui résulte à vérifier l'intégrité des données et l'authenticité de l'envoyeur.
- L'organisation receveuse retourne alors un récépissé signé à l'organisation envoyeuse sous la forme d'un message de notification de disposition de message. Ce récépissé signé va contenir le hachage de la signature provenant du message reçu, indiquant à l'envoyeur que le message reçu a été vérifié et/ou déchiffré correctement.

Cela décrit les fonctionnalités qui, si elles sont mises en œuvre, vont satisfaire toutes les exigences de sécurité. La présente spécification, laisse cependant une totale souplesse aux utilisateurs pour décider à quel degré ils veulent déployer ces caractéristiques de sécurité avec leurs partenaires commerciaux.

2.2.3 Définition des récipissés

Le terme utilisé aussi bien pour l'activité fonctionnelle que pour le message d'accusé de réception d'un échange EDI/EC est récipissé, ou récépissé signé. Le premier terme est utilisé si l'accusé de réception est pour un échange résultant en une réception qui N'EST PAS signée. Le second terme est utilisé si l'accusé de réception est pour un échange résultant en un récépissé qui EST signé. La méthode utilisée pour demander un récépissé ou un récépissé signé est définie dans la RFC2298, "Format de message extensible pour les notifications de disposition de message".

La "règle" est :

- Si un récipissé est demandé, spécifiant explicitement que le récipissé soit signé, le récipissé DOIT alors être retourné avec une signature.
- Si un récipissé est demandé, spécifiant explicitement que le récipissé soit signé, mais si le receveur ne peut pas prendre en charge le format du protocole ou les algorithmes de MIC demandés, un récépissé signé ou non signé DEVRAIT être retourné.
- Si une signature n'est pas explicitement demandée, ou si le paramètre de demande de récépissé signé n'est pas reconnu par l'UA, un récépissé peut être retourné ou non. Ce comportement est cohérent avec la MDN de la [RFC2298].

Un terme souvent utilisé en combinaison avec celui de récépissé est celui de "non répudiation de réception" (NRR, *Non-Repudiation of Receipt*). NRR se réfère à un événement légal qui ne survient que lorsque l'envoyeur d'origine d'un échange a vérifié le récépissé signé revenant de chez le receveur du message. Noter qu'une NRR n'est pas possible sans signature.

2.3 Hypothèses

2.3.1 Hypothèses de traitement d'EDI

- L'objet chiffré est un échange EDI
  La présente spécification suppose qu'un échange EDI normal est l'objet de plus bas niveau qui sera soumis aux services de sécurité.
  Dans le groupe de travail ANSI X12, cela signifie quelque chose entre, et incluant, les segments ISA et IEA. Dans EDIFACT, cela signifie quelque chose entre, et incluant, les segments UNA/UNB et UNZ. En d'autres termes, l'échange EDI incluant les segments d'enveloppe reste intact et non lisible durant le transport sécurisé.

- Les en-têtes d'enveloppe EDI sont chiffrés
  En cohérence avec la déclaration précédente, les en-têtes d'enveloppe EDI NE SONT PAS visibles dans le paquetage MIME. Afin d'optimiser l'acheminement à partir des réseaux d'EDI commerciaux existants (appelés réseaux à valeur ajoutée (VAN, *Value Added Network*) vers l'Internet, il reste à accomplir un travail de définition des

façons de tirer quelques informations de l'enveloppe pour les rendre visibles ; cependant, la présente spécification ne rentre dans aucun des détails de cette question.

- Considérations sur la sécurité de X12.58 et UN/EDIFACT
  Les organismes de normalisation les plus communs des EDI, ANSI X12 et EDIFACT, ont défini des dispositions internes pour la sécurité. X12.58 est le mécanisme de sécurité pour l'ANSI X12 et AUTACK fournit la sécurité pour EDIFACT. La présente spécification N'IMPOSE PAS l'utilisation ou la non utilisation de ces normes de sécurité. Elles sont toutes deux pleinement compatibles, bien qu'éventuellement redondantes, avec la présente spécification.

2.3.2 Hypothèses de souplesse

- Données chiffrées ou non
  La présente spécification permet des échanges de messages EDI où les données d'EDI peuvent être non protégées ou protégées au moyen du chiffrement.

- Données signées ou non signées
  La présente spécification permet un échange de messages d'EDI avec ou sans signature numérique de la transmission d'EDI d'origine.

- Utilisation ou non du récépissé
  La présente spécification permet une transmission de messages d'EDI avec ou sans demande de notification de réception. Cependant, si il est demandé une notification de réception signée, une valeur de mic est EXIGÉE au titre du récépissé retourné, sauf si survient une condition d'erreur dans laquelle une valeur de mic ne peut être retournée. En cas d'erreur, un récépissé non signé, ou une MDN, DEVRAIT être retourné avec la valeur correcte de "modificateur de disposition".

- Choix de formatages
  La présente spécification définit l'utilisation de deux méthodes pour formater les contenus d'EDI auxquels de la sécurité est appliquée.

- PGP/MIME-S/MIME
  La présente spécification s'appuie sur les lignes directrices établies dans les [RFC2015], [RFC3156] et [RFC2440] (PGP) et sur la syntaxe de format de message cryptographique des [RFC2630] et [RFC2633]. PGP/MIME ou S/MIME sont définis dans la présente déclaration d'applicabilité.

- Choix de fonction de hachage et de résumé de message
  Lorsque une signature est utilisée, il est RECOMMANDÉ que l'algorithme de hachage SHA1 soit utilisé pour tous les messages sortants, et que MD5 et SHA1 soient tous deux pris en charge pour les messages entrants.

En résumé, les huit permutations suivantes sont possibles dans toute relation d'affaires :
(1) l'envoyeur envoie des données non chiffrées, et ne demande pas de récipissé ;
(2) l'envoyeur envoie des données non chiffrées, et demande un reçu signé ou non signé. Le receveur renvoie le récépissé signé ou non signé ;
(3) l'envoyeur envoie des données chiffrées, et ne demande pas de récépissé ;
(4) l'envoyeur envoie des données chiffrées, et demande un récépissé signé ou non signé. Le receveur renvoie le récépissé signé ou non signé.
(5) L'envoyeur envoie des données signées, et ne demande pas de récépissé signé ou non signé.
(6) L'envoyeur envoie des données signées, et demande un récépissé signé ou non signé. Le receveur renvoie le récépissé signé ou non signé.
(7) l'envoyeur envoie des données chiffrées et signées, et ne demande pas de récépissé signé ou non signé.
(8) l'envoyeur envoie des données chiffrées et signées, et demande un récépissé signé ou non signé. Le receveur renvoie le récépissé signé ou non signé.

Note : Les usagers peuvent choisir l'une ou l'autre des huit possibilités, mais seul l'exemple (8), lorsque est demandé un récépissé signé, offre toute la suite des caractéristiques de sécurité décrites dans la "boucle de transmission sûre" mentionnée ci-dessus.

3. RFC référencées et leur apport

3.1 SMTP [RFC2821]

C'est la norme qui est au cœur du transfert de messagerie à laquelle tous les MTA doivent se conformer.

3.2 Format de message de texte [RFC0822]

Elle définit les champs d'en-tête de message et les parties qui constituent un message.

3.3 Multiparties de sécurité pour MIME [RFC1847]

Ce document définit les multiparties de sécurité pour MIME : multipart/encrypted et multipart/signed.

3.4 Multipartie/rapport [RFC1892]

Cette RFC définit l'utilisation du type de contenu multipart/report, sur la base duquel se construit la MDN de la [RFC2298].

3.5 Contenu d'EDI [RFC1767]

Cette RFC définit l'utilisation du type de contenu "application" pour ANSI X12 (application/EDI-X12), EDIFACT (application/EDIFACT) et les EDI définis mutuellement (application/EDI-Consent).

3.6 PGP/MIME [RFC2015], [RFC3156], [RFC2440]

Ces RFC définissent l'utilisation des types de contenu "multipart/encrypted", "multipart/signed", "application/pgp encrypted" et "application/pgp-signature" pour définir le contenu PGP MIME.

3.7 MIME [RFC2045], [RFC2046], et [RFC2049]

Ce sont les normes de base de MIME, sur lesquelles sont construites toutes les RFC qui se rapportent à MIME, y compris celle-ci. Les contributions clés incluent la définition du "type de contenu", du "sous-type" et de "multipartie", ainsi que les lignes directrices pour le codage, qui établissent l'US-ASCII à 7 bits comme jeu de caractères canonique à utiliser dans la messagerie Internet.

3.8 Notification de disposition de message[RFC2298]

Cette RFC définit comment une notification de disposition de message (MDN) est demandée, et le format et la syntaxe de la MDN. La MDN est la base sur laquelle les récipissés et les récipissés signés sont définis dans la présente spécification.

3.9 Spécifications de message S/MIME version 3 [RFC2633] et [RFC2630]

Ces spécification décrivent comment MIME doit transporter les objets de syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*).

4. Structure d'un message MIME EDI - Applicabilité

4.1 Introduction

Les structures ci-dessous sont décrites hiérarchiquement dans les termes des RFC qui sont appliquées pour former la structure spécifique. Pour les détails de la façon de coder conformément à toutes les RFC impliquées, se rapporter directement aux RFC référencées.

Aussi, ces structures décrivent seulement la transmission initiale. Les récipissés, et les demandes de récipissés sont traitées à la Section 5.

4.2 Structure d'un message EDI MIME - PGP/MIME

4.2.1 Pas de chiffrement, pas de signature

- RFC0822/2045
- RFC1767 (application/EDIxxxx ou /xml)

4.2.2 Pas de chiffrement, signature

- RFC0822/2045
- RFC1847 (multipartie/signé)
- RFC1767 (application/EDIxxxx ou /xml)
- RFC2015/2440/3156 (application/pgp-signature)

4.2.3 Chiffrement, pas de signature

- RFC822/2045
- RFC1847 (multipartie/chiffré)
- RFC2015/2440/3156 (application/pgp-chiffré) -"Version: 1"
- RFC2015/2440/3156 (application/flux d'octet)
- RFC1767 (application/EDIxxxx ou /xml) (chiffré)

4.2.4 Chiffrement, signature

- RFC822/2045
- RFC1847 (multipartie/chiffré)
- RFC2015/2440/3156 (application/pgp-chiffré) -"Version: 1"
- RFC2015/2440/3156 (application/flux d'octet)
- RFC1847 (multipartie/signé)(chiffré)
- RFC1767 (application/EDIxxxx ou /xml)(chiffré)
- RFC2015/2440/3156 (application/pgp-signature)(chiffré)

4.3 Structure d'un message EDI MIME - S/MIME

4.3.1 Pas de chiffrement, pas de signature

- RFC822/2045
- RFC1767 (application/EDIxxxx ou /xml)

4.3.2 Pas de chiffrement, signature

- RFC822/2045
- RFC1847 (multipartie/signé)
- RFC1767 (application/EDIxxxx ou /xml)
- RFC2633 (application/pkcs7-signature)

4.3.3 Chiffrement, pas de signature

- RFC822/2045
- RFC2633 (application/pkcs7-mime)
- RFC1767 (application/EDIxxxx ou /xml) (chiffré)

4.3.4 Chiffrement, signature

- RFC822/2045
- RFC2633 (application/pkcs7-mime)
- RFC1847 (multipart/signed) (encrypted)
- RFC1767 (application/EDIxxxx or /xml) (encrypted)
- RFC2633 (application/pkcs7-signature) (encrypted)

5. Récépissés

5.1 Introduction

Afin de prendre en charge la non répudiation de réception (NRR), un récépissé signé, sur la base de la signature numérique d'une notification de disposition de message, est à mettre en œuvre par l'agent d'utilisateur (UA, *User Agent*) du partenaire commercial receveur. La notification de disposition de message, spécifiée dans la [RFC2298] est signée numériquement par un partenaire commercial receveur au titre d'un message MIME multipartie/signé.

La prise en charge suivante des récépissés signés est EXIGÉE :
1) capacité à créer un multipartie/rapport; où le type de rapport = disposition-notification.
2) capacité de calculer une vérification d'intégrité de message (MIC, *Message Integrity Check*) sur le message reçu. La valeur de MIC calculée sera retournée à l'envoyeur du message au sein du récépissé signé.
4) capacité à créer un contenu multipartie/signé avec la notification de disposition de message comme première partie de corps, et la signature comme seconde partie de corps.
5) capacité de retourner le récépissé signé au partenaire commercial envoyeur.

Le récépissé signé est utilisé pour notifier au partenaire commercial envoyeur qui a demandé le récépissé signé que :
1) le partenaire commercial receveur accuse réception de l'échange d'EDI envoyé.
2) si le message envoyé était signé, le partenaire commercial envoyeur a alors authentifié l'envoyeur de l'échange d'EDI.
3) si le message envoyé était signé, le partenaire commercial envoyeur a alors vérifié l'intégrité de l'échange d'EDI envoyé.

Sans considérer si l'échange d'EDI était envoyé en format S/MIME ou PGP/MIME, l'UA du partenaire commercial receveur DOIT fournir le traitement de base suivant :
1) Si l'échange d'EDI envoyé est chiffré, la clé chiffrée symétrique et le vecteur d'initialisation (si applicable) sont déchiffrés en utilisant la clé privée du receveur.
2) La clé de chiffrement symétrique déchiffrée est alors utilisée pour déchiffrer l'échange d'EDI.
3) Le partenaire commercial receveur authentifie les signatures dans un message en utilisant la clé publique de l'envoyeur. L'algorithme d'authentification effectue ce qui suit :
   a) la vérification d'intégrité du message (MIC ou résumé de message) est déchiffrée en utilisant la clé publique de l'envoyeur.
   b) On calcule une MIC sur le contenu signé (l'en-tête MIME et l'objet EDI codé, conformément à la [RFC1767]) dans le message reçu en utilisant la même fonction de hachage unidirectionnelle que le partenaire commercial envoyeur.
   c) La MIC extraite du message envoyé, et la MIC calculée en utilisant la même fonction de hachage unidirectionnel que le partenaire commercial envoyeur sont comparés pour égalité.
4) Le partenaire commercial receveur formate la MDN et établit la MIC calculée dans le champ d'extension "MIC-de contenu-reçu".
5) Le partenaire commercial receveur crée un message MIME multipartie/signé conformément à la [RFC1847].
6) La MDN est la première partie du message multipartie/signé, et la signature numérique est créée sur cette MDN, y compris ses en-têtes MIME.
7) La seconde partie du message multipartie/signé contient la signature numérique. L'option "protocole" spécifiée dans la seconde partie du multipartie/signé est comme suit :
   S/MIME : protocole = "application/pkcs-7-signature"
   PGP/MIME : protocole = "application/pgp-signature"
8) Les informations de signature sont formatées conformément aux spécifications S/MIME ou PGP/MIME.

L'échange EDI et l'en-tête contenu EDI MIME de la RFC1767 peuvent en fait faire partie d'un type de contenu MIME multipartie. Lorsque l'échange EDI fait partie d'un type de contenu MIME multipartie, la MIC DOIT être calculée sur le contenu multipartie entier, y compris les en-têtes MIME.

La MDN signée, lorsque elle est reçue par l'envoyeur de l'échange EDI peut être utilisée par l'envoyeur :
1) comme une reconnaissance que l'échange EDI envoyé a été livré et acquitté par le partenaire commercial receveur. Le receveur fait cela en retournant l'identifiant du message d'origine du message envoyé dans la portion MDN du récépissé signé ;
2) comme une reconnaissance que l'intégrité de l'échange EDI a été vérifiée par le partenaire commercial receveur. Le receveur fait cela en retournant la MIC calculée de l'échange EDI reçu (et les en-têtes MIME de la RFC1767) dans le champ "MIC-du-contenu-reçu" de la MDN signée ;.
3) comme une reconnaissance que le partenaire commercial receveur a authentifié l'envoyeur de l'échange EDI ;
4) comme une non répudiation de réception lorsque la MDN signée est vérifiée avec succès par l'envoyeur avec la clé

publique du partenaire commercial receveur et que la valeur de la MIC retournée à l'intérieur de la MDN est la même que le résumé du message d'origine.

5.2 Demande d'un récépissé signé

Les notifications de disposition de message sont demandées conformément à la [RFC2298], "Format de message extensible pour les notifications de disposition de message". La demande que l'agent d'utilisateur receveur produise une notification de disposition de message est faite en plaçant l'en-tête suivant dans le message à envoyer :

MDN-request-header = "Disposition-notification-to" ":" mail-address

Le champ mail-address est spécifié comme une adresse usager@domaine de la [RFC0822], et est l'adresse de retour pour la notification de disposition de message.

En plus de demander une notification de disposition de message, une notification de disposition de message qui est signée numériquement, ou ce qui a été référencé comme un récépissé signé, peut être demandé en plaçant ce qui suit dans l'en-tête de message qui suit la ligne "Disposition-Notification-To".

Disposition-notification-options = "Disposition-Notification-Options" ":" disposition-notification-parameters
où
disposition-notification-parameters = parameter *(";" parameter)
où
parameter = attribute "=" importance ", " 1#value"
où
importance = "required" | "optional"

De sorte que la chaîne Disposition-notification-options pourrait être :

signed-receipt-protocol=optional, <protocol symbol>;
signed-receipt-micalg=optional, <micalg1>, <micalg2>,...;

Les valeurs actuellement prises en charge pour <protocol symbol> sont "pkcs7-signature", pour le format de signature S/MIME détachée, ou "pgp-signature", pour le format de signature pgp.

Les valeurs actuellement prises en charge pour l'algorithme de MIC sont :

Algorithme utilisé	**Valeur**
MD5	md5
SHA-1	sha1

(Note historique : certaines mises en œuvre anciennes de EDIINT émettaient et attendaient "rsa-md5" et "rsa-sha1" pour le paramètre micalg.) Les agents receveurs DEVRAIENT être capables de récupérer en douceur d'une valeur de paramètre micalg qu'ils ne reconnaissent pas.

Un exemple de ligne d'options formatée serait comme suit :

Disposition-notification-options:
signed-receipt-protocol=optional, pkcs7-signature;
signed-receipt-micalg=optional, sha1, md5

La sémantique du paramètre "signed-receipt-protocol" est la suivante :

1) Le paramètre "signed-receipt-protocol" est utilisé pour demander un récipissé signé au partenaire commercial receveur. Le paramètre "signed-receipt-protocol" spécifie aussi le format dans lequel le récépissé signé devrait être retourné au demandeur.
   Le paramètre "signed-receipt-micalg" est une liste d'algorithmes de MIC préférés par le demandeur pour les utiliser à la signature du récépissé retourné. La liste des algorithmes de MIC devrait être honorée par le receveur de gauche à droite.
   Les deux paramètres d'options "signed-receipt-protocol" et "signed-receipt-micalg" sont EXIGÉS lors de la demande d'un récépissé signé.

2) L'attribut "importance" de "Optional" est défini dans la MDN [RFC2298] et a la signification suivante :
Les paramètres avec une importance de "Optional" permettent à un UA qui ne comprend pas ce paramètre d'option particulier de générer quand même une MDN en réponse à une demande de MDN. Un UA qui ne comprend pas le paramètre "signed-receipt-protocol", ou le "signed-receipt-micalg" ne va évidemment pas retourner un récépissé signé.
L'importance de "Optional" est utilisée pour les paramètres récépissé signé parce qu'il est RECOMMANDÉ qu'une MDN soit retournée au partenaire commercial demandeur même si le receveur n'a pas pu le signer.
La MDN retournée va contenir des informations sur la disposition du message ainsi que pourquoi la MDN n'a pas pu être signée. Voir les détails du champ Disposition au paragraphe 5.3.
Au sein d'une relation commerciale d'EDI, si un récépissé signé est attendu et si il n'est pas retourné, il appartient alors aux partenaires commerciaux de résoudre le problème de la validité de la transaction. En général, si un récépissé signé est demandé dans la relation commerciale et si il n'est pas reçu, la transaction ne va vraisemblablement pas être considérée comme valide.

5.2.1 Considérations supplémentaires sur les récipissés signés

Les "règles" mentionnées au paragraphe 2.2.3 pour les récépissés signés sont les suivantes :

1) Lorsque un récépissé est demandé, spécifiant explicitement que le récépissé soit signé, le récépissé DOIT alors être retourné avec une signature.

2) Lorsque un récépissé est demandé, spécifiant explicitement que le récépissé soit signé, mais que le receveur ne peut pas prendre en charge soit le format de protocole demandé, soit les algorithmes de MIC demandés, un récépissé signé ou non signé DEVRAIT alors être retourné.

3) Lorsque une signature n'est pas explicitement demandée, ou lorsque le paramètre de demande de récépissé signé n'est pas reconnu par l'UA, aucun récépissé, un récépissé non signé, ou un récépissé signé PEUT être retourné par le receveur.

Note : Pour les EDI Internet, il est RECOMMANDÉ que lorsque une signature n'est pas explicitement demandée, ou si les paramètres ne sont pas reconnus, que l'UA renvoie au minimum un récépissé non signé. Si un récépissé signé a cependant toujours été retourné selon une politique, qu'il soit demandé ou non, alors tout faux récépissé non signé peut être répudié.

Lorsque est faite une demande de récépissé signé, mais qu'il y a une erreur dans le traitement du contenu du message, un récépissé signé DOIT quand même être retourné. La demande d'un récépissé signé DEVRA quand même être honorée, bien que la transaction elle-même puisse n'être pas valide. La raison pour laquelle le contenu n'a pas pu être traité DOIT être mise dans le champ "disposition".

Lorsque une demande de récépissé signé est faite, la "Received-content-MIC" DOIT toujours être retournée au demandeur. La "Received-content-MIC" DOIT être calculée comme suit :

- Pour tout message signé, la MIC à retourner est calculée sur le contenu et l'en-tête MIME [RFC1767]. La canonisation spécifiée dans la [RFC1848] DOIT être effectuée avant le calcul de la MIC, car l'envoyeur qui demande le récépissé signé était aussi REQUIS de canoniser.

- Pour les messages chiffrés, non signés, la MIC à retourner est calculée sur l'en-tête et le contenu MIME déchiffré [RFC1767]. Le contenu après déchiffrement DOIT être canonisé avant le calcul de la MIC.

- Pour les messages non signé, non chiffrés, la MIC DOIT être calculée sur le contenu du message avant le codage de transfert du contenu et sans les en-têtes MIME ou autres [RFC0822], car ils sont parfois altérés ou réarrangés par les MTA.

5.3 Format de notification de disposition de message

Le format d'une notification de disposition de message est spécifié dans la [RFC2298]. Pour l'usage des EDI Internet, le format suivant sera utilisé :
- type de contenu – selon les spécification de la [RFC1892] et de la [RFC2298]
- champ de rapport d'UA - selon la spécification de la [RFC2298]
- champ Passerelle MDN - selon la spécification de la [RFC2298]
- champ Receveur d'origine - selon la spécification de la [RFC2298]

- champ Receveur final - selon la spécification de la [RFC2298]
- champ Identifiant du message d'origine - selon la spécification de la [RFC2298]
- champ Disposition - les valeurs de "mode de disposition" suivantes DEVRAIENT être utilisées pour les EDI Internet :

"action automatique" La disposition décrite par le type de disposition résultait d'une action automatique, plutôt que d'une instruction explicite de l'usager pour ce message.
"action manuelle" La disposition décrite par le type de disposition résultait d'une instruction explicite de l'usager plutôt que d'une sorte d'action d'exécution automatique.
"Envoi MDN automatique" La MDN a été envoyée parce que l'UA avait été précédemment configuré à le faire.
"Envoi MDN manuel" L'usager a explicitement donné la permission d'envoi de cette MDN particulière. "Envoi MDN manuel" a du sens avec "action manuelle", mais pas avec "action automatique".

- champ disposition – les valeurs de "type de disposition" suivantes DEVRAIENT être utilisées pour les EDI Internet :

"traité" Le message a été traité d'une certaine façon (par exemple, imprimé, télécopié, transmis, transféré) sans être affiché à l'usager. Celui-ci peut ou non voir ultérieurement le message.
"échec" Un échec est survenu qui a empêché la bonne génération d'une MDN. Plus d'informations sur la cause de l'échec peuvent être contenues dans un champ Échec. Le type de disposition "échec" n'est pas à utiliser dans les situations dans lesquelles il y a des problèmes pour un traitement du message autre que d'interpréter la demande d'une MDN. Le type "traité" ou un autre type de disposition avec les modificateurs de disposition appropriés est à utiliser dans de telles situations.

- champ Disposition – les valeurs de "modificateur de disposition" suivantes DEVRAIENT être utilisées pour les EDI Internet :

"erreur" Une erreur qui est intervenue a empêché la réussite du traitement du message. Plus d'informations sont contenues dans un champ Erreur.
"avertissement" Le traitement du message a réussi mais une sorte de condition exceptionnelle s'est produite. Plus d'informations sont contenues dans un champ Avertissement.

5.3.1 Extensions de notification de disposition de message

Le "champ d'extension" suivant sera ajouté afin de prendre en charge les récépissés signés pour les types de contenu MIME de la [RFC1767] et les types de contenu MIME multiparties qui incluent le type de contenu MIME de la [RFC1767]. Le "champ d'extension" défini ci-dessus suit le "champ disposition" dans la MDN.

Le champ d'extension "MIC de contenu reçu" est établi lorsque l'intégrité du message reçu est vérifié. La MIC est la quantité codée en base64 qui est calculée sur le message reçu avec une fonction de hachage. Pour les détails de ce qui dans la "MIC de contenu reçu" devrait faire l'objet du calcul, voir le paragraphe 5.2.1. L'algorithme utilisé pour calculer la valeur de la "MIC de contenu reçu" DOIT être la même que la valeur de "micalg" utilisée par l'envoyeur dans le message multipartie/signé. Lorsque aucune signature n'est reçue, ou lorsque le paramètre mic-alg n'est pas accepté, il est alors RECOMMANDÉ que l'algorithme SHA1 soit utilisé pour calculer la MIC sur le message reçu ou le contenu du message.

Ce champ n'est établi que lorsque le traitement du contenu du message est mené à bien. Ce champ est utilisé en conjonction avec la signature du receveur sur la MDN afin que l'envoyeur vérifie la "non répudiation du récépissé".

- champ extension = "MIC de contenu reçu" ":" MIC

où :
<MIC> = <base64MicValue> "," <micalg>
<base64MicValue> = résultat d'une fonction de hachage unidirectionnelle, codée en base64.
<micalg> = valeur micalg définie dans la [RFC1847], jeton d'identifiant d'algorithme de MIC enregistré par l'IANA.

5.3.2 Utilisation du mode, type, et modificateur de disposition

On expose dans ce paragraphe les lignes directrices pour l'utilisation des champs "mode de disposition", "type de disposition", et "modificateur de disposition" dans les EDI Internet. Les champs "mode de disposition", "type de disposition", et "modificateur de disposition" sont décrits en détails dans la [RFC2298]. Les valeurs de "mode de disposition, "type de disposition" et "modificateur de disposition" DEVRAIENT être utilisées comme suit :

5.3.2.1 Traitement réussi

Lorsque l'UA receveur d'EDI a traité avec succès la demande d'un récépissé ou d'un récépissé signé, et le contenu du

message reçu, un récépissé ou une MDN DEVRAIT être retourné avec le "type de disposition" réglé à "il n'y a pas de moyen explicite pour qu'un usager contrôle l'envoi de la MDN", puis la première partie du "mode de disposition" devrait être réglé à "action automatique". Lorsque la MDN est envoyée sous le contrôle configurable de l'usager, la première partie du "mode de disposition" devrait alors être réglée à "action manuelle". Comme une demande de récépissé signé devrait toujours être honorée, il NE DOIT PAS être permis à l'usager de configurer l'UA à ne pas envoyer un récépissé signé lorsque l'envoyeur en demande un.

La seconde partie du "mode de disposition" est réglé à "Envoi MDN manuel" si l'usager a donné une permission explicite d'envoi de la MDN. Là encore, l'usager NE DOIT PAS être autorisé à refuser explicitement d'envoyer un récépissé signé lorsque l'envoyeur en demande un. La seconde partie du "mode de disposition" est réglé à "Envoi MDN automatique" chaque fois que l'UA EDI envoie automatiquement la MDN, sans considération de si l'envoi a été sous le contrôle d'un usager, d'un administrateur, ou d'un logiciel.

Comme un contenu d'EDI est généralement traité automatiquement par l'UA EDI, une demande de récépissé ou de récépissé signé va généralement retourner ce qui suit dans le "champ disposition" :

Disposition : action automatique/envoi MDN automatique; traité

Noter que la présente spécification ne restreint pas l'utilisation du "mode de disposition" aux seules actions automatiques. Les actions manuelles sont valides pour autant qu'on se souvienne qu'une demande de récépissé signé DOIT être honorée.

5.3.2.2 Contenu non traité

La demande d'un récépissé signé exige l'utilisation de deux "options de notification de disposition", qui spécifient le format protocolaire du récépissé signé retourné, et l'algorithme de MIC utilisé pour calculer la MIC sur le contenu du message. Les valeurs du "champ disposition" qui devraient être utilisées au cas où le contenu du message serait rejeté ou ignoré, par exemple, si l'UA EDI détermine qu'un récépissé signé ne peut pas être retourné parce qu'il ne respecte pas le format protocolaire demandé, de sorte que l'UA EDI choisit de ne pas traiter lui-même le contenu du message, devrait être spécifié dans le "champ disposition" de la MDN comme suit :

Disposition : "mode de disposition";
échec/Échec : format non accepté

La syntaxe du "type de disposition" "échec" est générale, permettant à l'envoyeur toute information textuelle avec le "type de disposition" "échec". Pour l'utilisation dans les EDI Internet, les valeurs de "échec" suivantes sont définies :

"Échec : format non accepté " "Échec :algorithmes de MIC non acceptés"

5.3.2.3 Erreurs du traitement du contenu

Lorsque des erreurs surviennent dans le traitement du contenu du message reçu, le "champ disposition" devrait être réglé à la valeur de "type de disposition" "traité" et la valeur de "modificateur de disposition" de "erreur". Pour l'utilisation dans les EDI Internet, les valeurs de "modificateur de disposition" de "erreur" suivantes sont définies :

- "Erreur : échec de déchiffrement" - le receveur n'a pas pu déchiffrer le contenu du message.
- "Erreur : échec d'authentification" - le receveur n'a pas pu authentifier l'envoyeur.
- "Erreur : échec de vérification d'intégrité" - le receveur n'a pas pu vérifier l'intégrité du contenu.
- "Erreur : erreur de traitement inattendue" – fourre-tout pour toutes les autres erreurs de traitement.

Un exemple de ce à quoi pourrait ressembler le "champ disposition" lorsque des erreurs de traitement du contenu sont détecté est le suivant :

Disposition : "mode de disposition";
Erreur de traitement : échec du déchiffrement

5.3.2.4 Avertissements sur le traitement du contenu

Il se trouve des situations dans les EDI où même si un partenaire commercial ne peut pas être authentifié correctement, les partenaires commerciaux sont quand même d'accord pour continuer le traitement des transactions d'EDI. La réconciliation des transactions est faite ultérieurement entre les partenaires commerciaux. Dans les situations d'avertissement sur le traitement du contenu décrites ci-dessus, le "champ disposition" DEVRAIT être réglé à la valeur de "type de disposition" de "traité", et à la valeur de "modificateur de disposition" de "avertissement". Pour l'utilisation

dans les EDI Internet, les valeurs de "modificateur de disposition" de "avertissement" suivantes sont définies :

"Avertissement : échec d'authentification, poursuite du traitement"

Un exemple de ce à quoi le "champ disposition" ressemblerait lorsque des avertissements sur le traitement du contenu sont détectés est le suivant :

Disposition : "mode de disposition"; traité/Avertissement : échec d'authentification, poursuite du traitement

5.4 Traitement de la notification de disposition de message

5.4.1 Traitement des gros dossiers

Les grands échanges d'EDI envoyés via SMTP peuvent être automatiquement fragmentés par des agents de transfert de message. Un sous-type de message/partiel, est défini dans la [RFC2045] pour permettre que de gros objets soient livrés en pièces séparés de messagerie et d'être automatiquement réassemblés par l'agent d'utilisateur receveur. Utiliser message/partiel, peut aider à alléger la fragmentation des grands messages par différents agents de transfert de message, mais n'élimine pas complètement le problème. Il est toujours possible qu'un morceau d'un message partiel, au moment du réassemblage, puisse se révéler contenir aussi un message partiel. Ceci est permis par les normes de l'Internet, et il est de la responsabilité de l'agent d'utilisateur de réassembler les morceaux fragmentés.

Il est RECOMMANDÉ que la taille de l'échange d'EDI envoyé via SMTP soit configurable afin que si la fragmentation est nécessaire, message/partiel puisse alors être utilisé pour envoyer le grand échange d'EDI en plus petits morceaux. La [RFC2045] définit l'utilisation de Content-Type: message/partial *(Type de contenu : message/partiel)*.

Note : La prise en charge du type de contenu message/partiel pour utilisation dans l'EDI Internet est FACULTATIVE et en l'absence de connaissance de sa prise en charge par le receveur NE DEVRAIT PAS être utilisée.

L'UA receveur est obligé de réassembler le message d'origine avant d'envoyer la notification de disposition de message à l'envoyeur d'origine du message. Une notification de disposition de message est utilisée pour spécifier la disposition du message envoyé entier, et ne devrait pas être retournée par un UA traitant tant que le message entier n'est pas reçu, même si le message reçu exige un réassemblage.

5.4.2 Exemple

Voici un exemple de récépissé signé retourné par un UA après le traitement réussi d'un type de contenu EDI MIME. Le partenaire commercial envoyeur a demandé le retour d'un récépissé signé.

Cet exemple suit le format S/MIME application/pkcs-7-signature.

Note : Cet exemple est donné comme simple illustration, et n'est pas considéré comme faisant partie de la spécification du protocole. Si un exemple entre en conflit avec les définitions du protocole spécifiées ci-dessus ou dans d'autres RFC référencées, c'est l'exemple qui est faux.

```
To: <recipient email>
Subject:
From: <sender email>
Date: <date>
Mime-Version: 1.0
Content-Type: multipart/signed; boundary="separator";
  micalg=sha1; protocol="application/pkcs7-signature"

 --separateur
& Content-Type:  multipart/report; report-type=disposition notification;  boundary="xxxxx"
&
& --xxxxx
& Content-Type: text/plain
&
& Le message envoyé au réceveur <Recipient@cyclonesoftware.com> a été reçu, l'échange EDI été bien déchiffré
& et son intégrité vérifiée. De plus, l'envoyeur du message, Sender <Edi_Sender@cyclonesoftware.com> a été
 & authentifié comme origine du message. Il n'est cependant pas garantit que l'échange d'EDI soit syntaxiquement
 & correct, ou ait été reçu par l'application d'EDI.
```

```
&
& --xxxxx
& Content-Type:  message/disposition-notification
&
& Reporting-UA: Interchange.cyclonesoftware.com (CI 2.2)
& Original-Recipient: rfc822; Edi_Recipient@cyclonesoftware.com
& Final-Recipient: rfc822;  Edi_Recipient@cyclonesoftware.com
& Original-Message-ID: <17759920005.12345@cyclonesoftware.com >
& Disposition: automatic-action/MDN-sent-automatically; processed
& Received-content-MIC: Q2hlY2sgSW50XwdyaXRIQ, sha1
&
& --xxxxx
& Content-Type: message/rfc822
&
& To: <recipient email>
& Subject:
&
&  [des champs d'en-tête supplémentaires viennent ici]
&
& --xxxxx--

  --separateur
  Content-Type: application/pkcs7-signature; name=smime.p7s;
  Content-Transfer-Encoding: base64
  Content-Disposition: attachment; filename=smime.p7s

  MIIHygYJKoZIhvcNAQcDoIIHuzCCB7cCAQAxgfIwge8CAQAwg
  ZgwgYMxFjAUBgNVBAMTDVRlcnJ5IEhhcmRpbmcxEDAOBgNVBA
  oTB0NZQ0xPTkUxDDAKBgNVBAsTA04vQTEQMA4GA1UEBxMHU=

--separateur--
```

Notes :

- Les lignes précédées d'une "&" sont celles sur lesquelles est calculée la signature.

(Pour les détails de la façon de préparer le multipartie/signé avec protocol = "application/pkcs7-signature" voir la "Spécification du message S/MIME, Services de sécurité PKCS pour MIME".)

Note : Comme spécifié par la [RFC1892], retourner le message original ou des portions du message original dans la troisième partie du corps du multipart/report n'est pas exigé. C'est une partie de corps facultative. Il est RECOMMANDÉ que les en-têtes reçus du message d'origine soient placés dans la troisième partie de corps, car ils peuvent être utilises pour retracer les problèmes.

Noter aussi que la première partie de corps textuelle du multipart/report peut être utilisée pour inclure une explication plus détaillés des conditions d'erreur rapportées par les en-têtes de disposition. La première partie de corps du multipart/report, lorsque elle est utilisée de cette façon, permet à une personne de mieux diagnostiquer les détails d'un problème.

6. Traitement du certificat de clé publique

6.1 Approche à court terme

À court terme, l'échange de clés publiques et la certification de ces clés doivent être traités au titre du processus d'établissement d'un partenariat commercial. L'UA et/ou l'interface d'application EDI doit tenir une base de données de clés publiques utilisées pour le chiffrement ou les signatures, en plus de la transposition entre l'identifiant de partenaire commercial d'EDI et une adresse de messagerie électronique de la [RFC0822]. Les procédures pour établir un partenariat commercial et pour configurer le système de messagerie d'EDI sécurisé peuvent varier selon les partenaires commerciaux et les paquetages logiciels.

Pour les systèmes qui utilisent les certificats X.509, il est RECOMMANDÉ que les partenaires commerciaux s'auto certifient l'un l'autre si ils n'utilisent pas une autorité de certification acceptée d'un commun accord. Il est fortement RECOMMANDÉ que lorsque des partenaires commerciaux utilisent S/MIME, ils échangent aussi les certificats de clé

publique en utilisant les recommandations spécifiées dans la spécification de message S/MIME version 3. Les formats de message et les exigences de conformité de S/MIME pour l'échange de certificat sont spécifiés dans le présent document.

Cette déclaration d'applicabilité N'EXIGE PAS l'utilisation d'une autorité de certification. L'utilisation d'une autorité de certification est donc FACULTATIVE.

6.2 Approche à long terme

À long terme, des normes Internet-EDI supplémentaires pourront être développées pour simplifier le processus d'établissement d'un partenariat d'affaires, incluant l'authentification par un tiers de partenaires commerciaux, ainsi que les attributs de la relation commerciale.

7. Considérations pour la sécurité

Ce document est entièrement consacré à la sécurité du transport des données d'affaires, et examine les questions de confidentialité et d'authentification.

Extrait de la spécification de message S/MIME version 2 :
Le chiffrement à 40 bits est considéré comme faible par la plupart des cryptographes. Utiliser un chiffrement faible n'offre que peu de sécurité réelle par rapport à l'envoi de texte en clair. Cependant, d'autres caractéristiques de S/MIME, comme la spécification de triple DES ou d'AES et la capacité à annoncer de plus fortes capacités cryptographiques aux partenaires de communication, permet aux envoyeurs de créer des messages qui utilisent un chiffrement fort. L'utilisation d'un chiffrement faible n'est jamais recommandée sauf comme alternative à pas de chiffrement du tout. Lorsque c'est faisable, les agents envoyeur et receveur devraient informer les envoyeurs et receveurs de la force relative du chiffrement des messages.

Extrait du traitement de certificat de S/MIME version 2 :
Lors du traitement de certificats, il y a de nombreuses situations où le traitement peut échouer. Comme le traitement peut être effectué par un agent d'utilisateur, une passerelle de sécurité, ou un autre programme, il n'y a pas une seule façon de traiter de telles défaillances. Le lecteur ne devrait pas conclure du fait que la liste des méthodes pour traiter les défaillances n'a pas été établie qu'elles ne sont pas importantes. C'est le contraire qui est vrai : si un certificat n'est pas d'une validité prouvée et associé au message, le logiciel de traitement devrait prendre des mesure immédiates et notables pour en informer l'utilisateur final.

Parmi les nombreux endroits où la vérification de signature et de certificat peut échouer, on citera :
- aucune chaîne de certificat ne conduit à un CA de confiance,
- pas de capacité à vérifier le CRL pour un certificat,
- un CRL invalide a été reçu,
- le CRL vérifié est arrivé à expiration,
- le certificat est arrivé à expiration,
- le certificat a été révoqué.

Il y a certainement d'autres instances dans lesquelles un certificat peut être invalide, et il est de la responsabilité du logiciel de traitement de les vérifier avec soin, et de décider de ce qu'il faut faire en cas d'échec de la vérification.

8. Remerciements

Un grand merci à l'auteur du précédent projet de l'IETF pour des EDI sécurisés sur la base de MIME : Mats Jansson.

Les auteurs doivent des remerciements particuliers à Carl Hage, Jun Ding, Dale Moberg, et Karen Rosenthal qui ont fourni à notre équipe des retours précieux et très complets. Sans leur participation, nos efforts auraient eu du mal à aboutir d'une façon utile pour les usagers et les développeurs de cette technologie.

De plus, les auteurs tiennent à remercier Harald Alvestrand, Jim Galvin, et Roger Fajman de leurs conseils et apports.

9. Références

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC1767] D. Crocker,"Encapsulation MIME d'objets d'échange de données informatisées", mars 1995. *(P.S.)*

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC1892] G. Vaudreuil, "Type de contenu multipart/rapport pour les rapports de messages administratifs de systèmes de messagerie", janvier 1996. *(Obsolète, voir* RFC3462*) (P.S.)*

[RFC2015] M. Elkins, "Sécurité de MIME avec Pretty Good Privacy (PGP)", octobre 1996. (*MàJ par* RFC3156*) (P.S.)*

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par 2184, 2231, 5335.)*

[RFC2046] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 2 : Types de support", novembre 1996. *(D. S., MàJ par* 2646, 3798, 5147, 6657*.)*

[RFC2049] N. Freed, N. Borenstein, "Extensions multi-objets de la messagerie Internet (MIME) Partie cinq : critères de conformité et exemples", novembre 1996. *(Remplace* RFC1521, RFC1522, RFC1590*) (D.S.)*

[RFC2298] R. Fajman, "Format de message extensible pour les notifications de disposition de message", mars 1998. (*Obsolète, voir* RFC3798*) (P.S.)*

[RFC2440] J. Callas, L. Donnerhacke, H. Finney et R. Thayer, "Format de message OpenPGP", novembre 1998. *(Obsolète, voir* RFC4880*)*

[RFC2630] R. Housley, "Syntaxe de message cryptographique", juin 1999. *(Obsolète, voir* 3369, 3370*) (P.S.)*

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC2821] J. Klensin, éditeur, "Protocole simple de transfert de messagerie", STD 10, avril 2001. *(Obsolète, voir* RFC5321*)*

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822*, STD 11, Remplacée par* RFC5322*)*

[RFC3156] M. Elkins et autres, "Sécurité MIME avec OpenPGP", août 2001.*(P.S.)*

Appendice Formulaire d'enregistrement auprès de l'IANA

A.1 Enregistrement par l'IANA du paramètre de disposition de contenu signed-receipt-protocol

Nom de paramètre : signed-receipt-protocol
Syntaxe : voir au paragraphe 5.2 du présent document.
Spécification : voir au paragraphe 5.2 du présent document.

A.2 Enregistrement par l'IANA du paramètre de disposition de contenu signed-receipt-micalg

Nom de paramètre : signed-receipt-micalg
Syntaxe : voir au paragraphe 5.2 du présent document.
Spécification : voir au paragraphe 5.2 du présent document.

A.3 Enregistrement par l'IANA du nom de champ d'extension MDN Received-content-MIC

Nom de champ d'extension : Received-content-MIC
Syntaxe : voir au paragraphe 5.3.1 du présent document.
Spécification : voir au paragraphe 5.3.1 du présent document.

Adresse des auteurs

Terry Harding
Cyclone Commerce
8388 E. Hartford Drive
Scottsdale, Arizona 85255, USA
mél : tharding@cyclonecommerce.com

Chuck Shih
Gartner Group
251 River Oaks Parkway
San Jose, CA 95134-1913 USA
mél : chuck.shih@gartner.com

Rik Drummond
Drummond Group
P.O. Box 101567
Ft. Worth, TX 76105 USA
mél : rik@drummondgroup.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.