GS1 France

The Global Language of Business

Modèle d'Accord d'Interchange

Echange de Données Informatisé

(EDI)

Version 1

2009

1 PREAMBULE

Le commerce électronique offre de nouvelles possibilités d'accroître l'efficacité des opérations commerciales et de réduire les coûts liés aux procédures commerciales en procurant des avantages concurrentiels plus importants aux participants prêts à adopter de nouvelles méthodes de travail et de nouveaux moyens de commercer.

Les nouveaux moyens qui se mettent en place pour le commerce électronique et l'utilisation d'Internet offrent aux utilisateurs un ensemble de technologies leur permettant de communiquer des données, de conclure des contrats par voie électronique et de gérer de nouveaux processus professionnels débouchant sur de nouveaux modèles de transactions.

Cet accord d'interchange comprend l'accord proprement dit, une annexe technique, ainsi qu'une annexe fonctionnelle. Cet accord intervient entre deux partenaires EEP (Echanges Electroniques Professionnels peuvent se définir comme étant les activités nécessaires à l'échange d'information de système d'information à système d'information sans intervention humaine). Il fixe les conditions générales des échanges EEP. Il ne préjuge pas des contrats existants entre les partenaires et leurs réseaux à valeur ajoutée ou leurs fournisseurs de progiciels pour les EEP. Afin de vous aider dans la compréhension des termes techniques utilisés dans ce document, un glossaire à été ajouté. Il n'est pas nécessaire de transmettre ce glossaire dans votre accord d'interchange.

Cet accord peut être soit établi entre les parties, soit annexé à un contrat.

2 DESCRIPTIF

ENTRE :
Ci-après dénommée " Partenaire 1 "
Société.....
.....
Siège : .....
.....
….....

ET :
Ci-après dénommée " Partenaire 2 "
Société.....
.....
Siège : .....
.....
.....

2.1 Objet et portée

L'accord d'interchange concerne les transferts de messages entre les partenaires effectuant des transactions commerciales au moyen des EEP.
Il comprend l'accord proprement dit, une annexe technique fonctionnelle, et fixe les conditions générales des échanges EEP.

L'annexe technique contient tous les éléments concernant la mise en œuvre opérationnelle des télécommunications entre les partenaires, réseaux, adresses réseaux, horaires. Si plusieurs réseaux ou

stations EEP sont utilisés, il peut être nécessaire d'établir autant d'annexes techniques qu'il y a de réseaux ou de stations EEP.

L'annexe fonctionnelle définit les messages et leurs utilisations.

Les annexes sont datées et susceptibles d'être mises en jour. Elles peuvent évoluer dans le temps. Toutefois, l'accord ne traite pas des conséquences juridiques des transactions conclues par EEP.

2.2 Exigences et spécifications techniques

Sont inclus dans les annexes, les matières opérationnelles suivantes :

- les équipements utilisés, les moyens de communication, les messages standard et les accords de codification ;
- les modalités de traitement et d'accusé de réception des messages ;
- la sécurité des messages ;
- les enregistrements et la conservation desmessages ;
- la planification de mise en œuvre et les tests éventuels.

2.3 Exigences opérationnelles

Les partenaires s'engagent à se doter et à maintenir les équipements et logiciels informatiques. Les détails concernant les réseaux, les moyens de connexion, ainsi que ceux concernant les messages, leurs versions et leurs utilisations sont décrits dans les annexes techniques et fonctionnelles.

2.4 Modalités de traitement et d'accusé de réception des messages

Les messages reçus doivent être traités aussi vite que possible et, le cas échéant dans le délai fixé par l'annexe technique.

Si un accusé de réception est requis, sa nature est précisée dans l'annexe technique. La réception de cet accusé par l'émetteur lui garantit la prise en compte du message par le destinataire, mais elle n'équivaut pas à une acceptation du contenu.

2.5 Enregistrement et conservation des données

Afin de garantir la sécurité des échanges, des délais de conservation des messages échangés peuvent être définis. Ces délais permettent d'assurer les retraitements ou les réémissions des messages. Ces délais doivent au moins couvrir le temps nécessaire à la conclusion des transactions concernées. Ils seront précisés dans l'annexe technique, message par message si nécessaire.

Des obligations d'archivage sont également fixées dans le cadre de la dématérialisation fiscale, (article 8). Les durées d'enregistrement ou de conservation des données définies par le présent accord concernent le processus EEP ; elles ne remettent pas en cause l'obligation faite par le droit commercial de conserver la preuve des transactions pendant 10 ans.

2.6 Maintenance et évolution de l'accord

Afin de tenir compte des évolutions techniques ou commerciales, les parties s'engagent à maintenir à jour les annexes techniques et fonctionnelles. Les modifications doivent être notifiées avec un préavis de _____ mois.
Elles ne peuvent entrer en application qu'après la validation par les parties des tests préalables à la mise en œuvre opérationnelle.

2.7 Validité des messages fiscaux

Dans le cadre de la dématérialisation fiscale, les partenaires s'accordent sur les compléments matériels et logiciels nécessaires.

Pour les factures, les avoirs, les notes de débit ou de crédit échangés entre partenaires français ayant adopté la dématérialisation fiscale de la facture, le délai minimum de conservation est de 3 ans sur support magnétique. Ce délai doit être complété par une période complémentaire de 3 ans sur tout autre support.

Se référer à la dernière version du guide des bonnes pratiques "dématérialisation de la facture (Dispositions communes aux deux procédures de transmission par voie électronique)" de GS1 France.

2.8 Durée des dispositions de l'accord

Le présent accord sera considéré comme étant effectif à compter de sa signature et jusqu'à son éventuel résiliation.

2.9 Informatique et liberté

Le cas échéant, les parties s'engagent à respecter les dispositions légales et réglementaires concernant la constitution et l'exploitation de fichiers regroupant les données nominatives.

Fait à _____
Le _____

Partenaire 1 (cachet de la société)
Nom du signataire :.....
Qualité :.....

Partenaire 2 (cachet de la société)
Nom du signataire :.....
Qualité :.....

3 ANNEXE TECHNIQUE, VERSION : _____ DATE : _____

3.1 Types de langages utilisés

Les partenaires précisent ici le(s) type(s) de langage(s) utilisé(s) :
☐ EANCOM ☐ GENCOD ☐ XML

3.2 Types d'échanges

Les partenaires précisent ici le(s) type(s) d'échange(s) utilisé(s) :

Partenaire 1
☐EDI conventionnel ☐ WEB-EDI/EFI

Partenaire 2
☐ EDI conventionnel ☐ WEB-EDI/EFI

3.3 Protocoles de communication

Les partenaires précisent ici le(s) protocole(s) utilisé(s) :

Partenaire 1
☐ RVA (X400, FTP) ☐ AS2

Partenaire 2
☐ RVA (X400, FTP) ☐ AS2

3.3.1 Pré-requis au protocole X400, FTP

Les partenaires s'engagent à mettre en place l'organisation nécessaire à la sécurité des données dans leur système interne et selon leur configuration, à savoir :
Confidentialité, Authentification, Intégrité, Non-répudiation

3.3.1.1 Réseaux de communication

Les partenaires précisent ici le(s) réseau(x) utilisé(s) ainsi que leurs ordres de priorité.

Partenaire 1

Le(s) réseau(x) utilisé(s) par ordre de priorité est (sont) :

☐ Allegro (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ Atlas 400 (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ IBM (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Partenaire 2

☐ Allegro (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ Atlas 400 (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ IBM (RVA)
Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ Autre RVA, à préciser : _____

Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

☐ Autre RVA, à préciser : _____

Adresse réseau (BAL) (test) :
_____
_____

Adresse réseau (BAL) (production) :
_____
_____

3.3.1.2 Logiciel de télécommunication

Les partenaires précisent ici le logiciel de télécommunication.

Partenaire 1

☐ Allegro version _____
☐ Serveur privé _____

pour un autre logiciel de
télécommunication préciser :
_ son nom _____
_ sa version _____
_ le matériel _____

Partenaire 2

☐ Allegro version _____
☐ Serveur privé _____

pour un autre logiciel de
télécommunication préciser :
_ son nom _____
_ sa version _____
_ le matériel _____

3.3.1.3 Traducteur, WEB EDI/EFI

Partenaire 1

Le traducteur utilisé est :
_____
Il a été :
☐ développé en interne
☐ acheté/hébergé auprès de _____

Le fournisseur d'accès au WEB EDI/EFI est :
est :
_____

Partenaire 2

Le traducteur utilisé est :
_____
Il a été :
☐ développé en interne
☐ acheté/hébergé auprès de _____

Le fournisseur d'accès au WEB EDI/EFI

_____

3.3.1.4 Contacts X400, FTP

Précisez les informations relatives aux contacts X400, FTP.

Partenaire 1
- Nom de l'interlocuteur : _____
- Fonction : _____
- Service / département : _____
_____
- Tél : _____
- Fax : _____
- E-mail : _____

Partenaire 2
- Nom de l'interlocuteur : _____
- Fonction : _____
- Service / département : _____
_____
- Tél : _____
- Fax : _____
- E-mail : _____

- Adresse postale :
_____
_____
_____
_____

- Adresse postale :
_____
_____
_____
_____

3.3.1.5 Procédures de secours

En cas de dysfonctionnement, les procédures de secours peuvent être spécifiques à chaque entreprise.

Partenaire 1

Les procédures de secours mises en œuvre sont :

_ En cas d'indisponibilité du réseau Prioritaire (l'ordre de priorité est défini dans 3.3.1.1)

_ En cas d'indisponibilité du ou des réseaux :

- Fax : _____
- Tél : _____
- E-mail : _____
- Station de secours : _____

_ En cas de dysfonctionnement, une procédure de secours assure une reprise dans un délai de ____ heures, pour les messages d'une antériorité de _____ heures.

Partenaire 2

_ En cas d'indisponibilité du réseau prioritaire (l'ordre de priorité est défini dans 3.3.1.1)

_ En cas d'indisponibilité du ou des réseaux :

- Fax : _____
- Tél : _____
- E-mail : _____
- Station de secours : _____

_ En cas de dysfonctionnement, une procédure de secours assure une reprise dans un délai de ____ heures, pour les messages d'une antériorité de _____ heures.

3.3.1.6 Horaires et fréquences des échanges

Partenaire 1

Dépose et retire ses messages *aux fréquences suivantes* :

Message _____ en
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

Message _____
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

Partenaire 2

Dépose et retire ses messages *aux fréquences suivantes* :

Message _____ en
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

Message _____
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

Tous messages en :
☐ Emission ☐ Réception

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____
____h et ____h __ Min _____

Remarque :
Ces horaires peuvent être définis par type de message si les partenaires le jugent nécessaire.

3.3.1.7 Indisponibilité des échanges

Précisez les jours et les heures d'indisponibilités des stations et des systèmes d'informations.

Partenaire 1

_____
_____
_____
_____
_____
_____
_____
_____

Partenaire 2

_____
_____
_____
_____
_____
_____
_____
_____

3.3.1.8 Réception

L'interchange est considéré comme réceptionné après le retour de l'accusé réception (réseaux, station ou applicatif).

3.3.1.9 Signaux d'alerte

L'entreprise émettrice devra alerter son partenaire si l'accusé n'est pas reçu dans un délai de _____ après l'émission des messages.

Elle contactera alors par téléphone l'utilisateur de la station chez l'autre partie.

3.3.1.10 Tests et montée en charge

Après la période de tests techniques, les échanges en réel débutent après accord entre les parties.

Dans le cas particulier du message commande, il est prévu d'appliquer pendant un délai de ___ jours ou à l'occasion _____ échanges, une procédure en double du message EDI avec le mode d'échange appliqué précédemment.

Pendant la période de tests, les partenaires peuvent convenir d'utiliser une boîte aux lettres de tests, ou un GLN de tests. Cette procédure peut s'avérer très utile pour la mise en place d'un nouveau message venant s'ajouter à des messages déjà opérationnels.

3.3.2 Pré-requis au protocole AS2

Pour remplir cette partie, merci de bien vouloir se référer au "guide français d'utilisation du protocole AS2" GS1 France.

Les partenaires s'engagent à mettre en place l'organisation nécessaire à la sécurité des données dans leur système interne et selon leur configuration, à savoir :
Confidentialité, Authentification, Intégrité, Non-répudiation

Partenaire 1
Le protocole de communication utilisé est :
☐ HTPP
☐ HTPP(S)

Partenaire 2
Le protocole de communication utilisé est :
☐ HTPP
☐ HTPP(S)

- **Données d'en-tête AS2**

AS2To GLN : _____

AS2From GLN : _____

- . **Certificats**

Partenaire 1
☐ *Signature électronique*
Garantie des certificats

Classe 2 : Le certificat est délivré après l'interrogation d'une base de données et la récupération de pièces administratives (cartes d'identité des dirigeants et K-BIS de l'entreprise demandant le certificat)

Type de certificats en production "Trusted"

Type de certificats en test
☐ Trusted ☐ Self-signed

Acteurs relatifs au certificat
Détenteur de la clé : _____

Autorité d'enregistrement :
☐ GENDI ☐ GENFA ☐ GS1 France

Autorité de certification : GS1 France

Opérateur -Tiers certificateur :
CERTEUROPE

Partenaire 2
☐ *Signature électronique*
Garantie des certificats

Classe 2 : Le certificat est délivré après l'interrogation d'une base de données et la récupération de pièces administratives (cartes d'identité des dirigeants et K-BIS de l'entreprise demandant le certificat)

Type de certificats en production "Trusted"

Type de certificats en test
☐ Trusted ☐ Self-signed

Acteurs relatifs au certificat
Détenteur de la clé : _____

Autorité d'enregistrement :
☐ GENDI ☐ GENFA ☐ GS1 France

Autorité de certification : GS1 France

Opérateur -Tiers certificateur :
CERTEUROPE

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Algorithme de signature électronique
SHA1 (Secure Hash Algorithm version 1)

Longueur des clés publiques,
privés _____ bits (minimum 128 bits)

☐ *Cryptage*

Garantie des certificats

Classe 2 : Le certificat est délivré après l'interrogation d'une base de données et la récupération de pièces administratives (cartes d'identité des dirigeants et K-BIS de l'entreprise demandant le certificat)

Type de certificats en production
"Trusted"

Type de certificats en test
☐ Trusted ☐ Self-signed

Acteurs relatifs au certificat

Détenteur de la clé : _____
Autorité d'enregistrement :
☐ GENDI ☐ GENFA ☐ GS1 France

Autorité de certification : GS1 France

Opérateur -Tiers certificateur :
CERTEUROPE

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Algorithme de signature électronique
SHA1 (Secure Hash Algorithm version 1)

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Algorithme de signature électronique
SHA1 (Secure Hash Algorithm version 1)

Longueur des clés publiques,
privés _____ bits (minimum 128 bits)

☐ *Cryptage*

Garantie des certificats

Classe 2 : Le certificat est délivré après l'interrogation d'une base de données et la récupération de pièces administratives (cartes d'identité des dirigeants et K-BIS de l'entreprise demandant le certificat)

Type de certificats en production
"Trusted"

Type de certificats en test
☐ Trusted ☐ Self-signed

Acteurs relatifs au certificat

Détenteur de la clé : _____
Autorité d'enregistrement :
☐ GENDI ☐ GENFA ☐ GS1 France

Autorité de certification : GS1 France

Opérateur -Tiers certificateur :
CERTEUROPE

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Validité du certificat
_____ ans (minimum 2 ans)
_____ ans (maximum 5 ans)

Algorithme de signature électronique
SHA1 (Secure Hash Algorithm version 1)

Longueur des clés publiques,
privés _____ bits (minimum 128 bits)

Longueur des clés publiques,
privés _____ bits (minimum 128 bits)

- . **Accusé de réception des fichiers**

Acquittement de la réception des fichiers est réalisé par l'envoi du MDN à la réception complète des données

Partenaire 1
Accusé de transport "Signé"

Mode de transmission
☐ Synchrone ☐ Asynchrone

Horodatage
☐ Non utilisé ☐ Utilisé

Partenaire 2
Accusé de transport "Signé"

Mode de transmission
☐ Synchrone ☐ Asynchrone

Horodatage
☐ Non utilisé ☐ Utilisé

- . **Format du message relatif au protocole**

Partenaire 1
Type de format message "S/MIME"
Compression des données (ZLIB)
☐ Obligatoire
☐ Acceptée et facultative
☐ Non-acceptée

Partenaire 2
Type de format message "S/MIME"
Compression des données (ZLIB)
☐ Obligatoire
☐ Acceptée et facultative
☐ Non-acceptée

3.3.2.1 Réseaux

Les partenaires précisent ici le(s) réseau(x) utilisé(s).

Partenaire 1
Le(s) réseau(x) utilisé(s) est (sont) :
☐ Internet
☐ Autre, à préciser : _____

Adresse réseau (URI) (test) :
_____
_____

Adresse réseau (URI) (production) :
_____
_____

Adresse réseau (IP) (test) :
_____
_____

Adresse réseau (IP) (production) :
_____
_____

Pour HTPPS, vous devez préciser :
Nom utilisateur :_____
Mot de passe : _____

Partenaire 2
Le(s) réseau(x) utilisé(s) est (sont) :
☐ Internet
☐ Autre, à préciser : _____

Adresse réseau (URI) (test) :
_____
_____

Adresse réseau (URI) (production) :
_____
_____

Adresse réseau (IP) (test) :
_____
_____

Adresse réseau (IP) (production) :
_____
_____

Pour HTPPS, vous devez préciser :
Nom utilisateur :_____
Mot de passe : _____

Le(s) réseau(x) utilisé(s) est (sont) :
☐ Internet
☐ Autre, à préciser : _____

Le(s) réseau(x) utilisé(s) est (sont) :
☐ Internet
☐ Autre, à préciser : _____

3.3.2.2 Logiciel de communication

Les partenaires précisent ici le logiciel de communication.

Partenaire 1
- son nom _____
- sa version _____
- le matériel _____

Partenaire 2
- son nom _____
- sa version _____
- le matériel _____

3.3.2.3 Traducteur, Web EDI/EFI

Partenaire 1
Le traducteur utilisé est :

_____

Il a été :
☐ développé en interne
☐ acheté/hébergé auprès de _____

Le fournisseur d'accès au WEB EDI/EFI est : _____

Partenaire 2
Le traducteur utilisé est :

_____

Il a été :
☐ développé en interne
☐ acheté/hébergé auprès de _____

Le fournisseur d'accès au WEB EDI/EFI est : _____

3.3.2.4 Contacts AS2

Précisez les informations relatives aux contacts AS2.

Partenaire 1
- Nom de l'interlocuteur : _____
- Fonction : _____
- Service / département : _____
_____
- Tél : _____
- Fax : _____
- E-mail : _____
- Adresse postale :
_____
_____
_____
_____

Partenaire 2
- Nom de l'interlocuteur : _____
- Fonction : _____
- Service / département : _____
_____
- Tél : _____
- Fax : _____
- E-mail : _____
- Adresse postale :
_____
_____
_____
_____

3.3.2.5 Procédures de secours

En cas de dysfonctionnement, les procédures de secours peuvent être spécifiques à chacune entreprise.

Partenaire 1
Les procédures de secours mises en œuvre sont :

_ En cas d'indisponibilité du réseau défini en 3.3.2.1), précisez le nom du Réseau à Valeur Ajouté ainsi que l'adresse de la boite aux lettres (BAL) :

Partenaire 2
Les procédures de secours mises en œuvre sont :

_ En cas d'indisponibilité du réseau défini en 3.3.2.1), précisez le nom du Réseau à Valeur Ajouté ainsi que l'adresse de la boite aux lettres (BAL) :

Réseau : _____
Adresse réseau (BAL) :
_____
_____
_____

_ En cas d'indisponibilité du ou des réseaux :

- Fax : _____
- Tél : _____
- E-mail : _____
- Station de secours : _____

_ En cas de dysfonctionnement, une procédure de secours assure une reprise dans un délai de ____ heures, pour les messages d'une antériorité de _____ heures.

Réseau : _____
Adresse réseau (BAL) :
_____
_____
_____

_ En cas d'indisponibilité du ou des réseaux :

- Fax : _____
- Tél : _____
- E-mail : _____
- Station de secours : _____

_ En cas de dysfonctionnement, une procédure de secours assure une reprise dans un délai de ____ heures, pour les messages d'une antériorité de _____ heures.

3.3.2.6 Horaires et fréquences des échanges

Précisez les jours et les heures d'indisponibilités des stations et des systèmes d'informations.

Partenaire 1

Dépose et retire ses messages *aux fréquences suivantes* :

Message _____ en
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

Message _____
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

Tous messages en :
☐ Emission ☐ Réception

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

Partenaire 2

Dépose et retire ses messages *aux fréquences suivantes* :

Message _____ en
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

Message _____
☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

☐ *Emission* ☐ *Réception*

Période Fréquence Jour
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____
____*h et* ____*h* __ *Min* _____

Remarque :
Ces horaires peuvent être définis par type de message si les partenaires le jugent nécessaire.

3.3.2.7 Indisponibilité des échanges

Précisez les jours et les heures d'indisponibilités des stations et des systèmes d'informations.

Partenaire 1	**Partenaire 2**
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

3.3.2.8 Réception

L'interchange est considéré comme réceptionné après le retour de l'accusé réception (réseaux, passerelle, station ou applicatif).

3.3.2.9 Signaux d'alerte

L'entreprise émettrice devra alerter son partenaire si l'accusé n'est pas reçu dans un délai de _____ après l'émission des messages.

Elle contactera alors par téléphone l'utilisateur de la station chez l'autre partie.

3.3.2.10 Tests et montée en charge

Après la période de tests techniques, les échanges en réel débutent après accord entre les parties.

Dans le cas particulier du message commande, il est prévu d'appliquer pendant un délai de ___ jours ou à l'occasion _____ échanges, une procédure en double du message EDI avec le mode d'échange appliqué précédemment.

Pendant la période de tests, les partenaires peuvent convenir d'utiliser une plate-forme de tests, ou un GLN de tests. Cette procédure peut s'avérer très utile pour la mise en place d'un nouveau message venant s'ajouter à des messages déjà opérationnels.

4 ANNEXE FONCTIONNELLE, VERSION : _____ DATE : _____

4.1 Messages échangés

Dans le cadre du présent accord d'interchange EEP, les partenaires conviennent d'échanger des messages (commerciaux, finance, service, transport, etc..) en respectant les accords d'utilisation précisées dans le tableau ci-dessous.

Messages	**Intégration automatique du message dans votre applicatif**	**GENCOD (message, version)**	**EANCOM 97 (message, version)**	**XML (message, Version du standard EAN.UCC)**	**Autres**
Information Produit	*NON (*)*		*PRODAT D96A EAN008 (*)*	*ITEM 1.3.1 (*)*	
Information partenaires					
Commande	*OUI (*)*	*023 V4 (*)*			
Livraison					
Accusé de réception syntaxique			*CONTRL D96A EAN008 (*)*		
Accusé de réception applicatif			*APERAK D96A EAN008 (*)*		
.....					

(*) : fourni à titre d'exemple

En plus de ce tableau, les partenaires peuvent définir un scénario de flux visant à préciser l'enchaînement des messages entre eux. Il sera précisé dans un autre document, par exemple, les conditions générales d'achat).

4.2 Contacts Messages

Messages	**Partenaire 1**	**Partenaire 2**
Information Produit (*)	_ Nom de l'interlocuteur : _____ _____ _____ _ Fonction : _____ _ Service / département : _____ _____ _____ _ Tél : _____ _ Fax : _____ _ E-mail : _____	_ Nom de l'interlocuteur : _____ _____ _____ _ Fonction : _____ _ Service / département : _____ _____ _____ _ Tél : _____ _ Fax : _____ _ E-mail : _____

	_ Adresse postale : _____ _____ _____	_ Adresse postale : _____ _____ _____
Tous types de messages (*)	_ Nom de l'interlocuteur : _____ _____ _____ _ Fonction : _____ _ Service / département : _____ _____ _____ _ Tél : _____ _ Fax : _____ _ E-mail : _____ _ Adresse postale : _____ _____ _____	_ Nom de l'interlocuteur : _____ _____ _____ _ Fonction : _____ _ Service / département : _____ _____ _____ _ Tél : _____ _ Fax : _____ _ E-mail : _____ _ Adresse postale : _____ _____ _____

(*) : fourni à titre d'exemple

4.3 Codification

Pour identifier les articles ou les produits, objets de leurs échanges, les parties conviennent d'utiliser les standards EAN.UCC d'identification des unités consommateurs (GTIN) et des unités logistiques (GTIN, SSCC dans les messages adéquates).
Pour identifier les partenaires et leurs fonctions dans les messages, les parties conviennent d'utiliser les GLN.
L'utilisation des codes résultant de ces systèmes de codification nécessite la communication préalable de données, sous forme de fiche-produit, de déclaration de GLN et de filières. Cette communication peut se faire selon des modes qui doivent être précisés par les partenaires en annexe : papier, disquette, message EEP, consultation de base de données.

4.4 Profils d'utilisation des messages

Dans le respect du standard retenu au chapitre "Messages échangés", les partenaires définissent des profils utilisateurs des messages. Ces profils ont pour but de préciser les données compatibles avec les logiciels applicatifs et les bases de données des deux partenaires. Pour les messages qui ne sont pas soumis à des restrictions, la seule référence au standard suffit. Dans le cas contraire, la description précise du profil doit être jointe au présent accord.

5 GLOSSAIRE

Termes Définitions

AS2 Acronyme de "Applicability Statement 2".
C'est une spécification dédiée aux échanges de données informatisés entre les entreprises exploitant le protocole HTTP (Hypertext Transfer Protocol), connu pour permettre la transmission des pages Web. Cette spécification est une évolution d'AS1 et a été conçue dans le cadre du groupe de travail EDIINT (EDI via Internet), lié à l'IETF (Internet Engineering Task Force), qui développe des standards de communication répondant à des objectifs de fiabilité et de sécurisation. Voir le guide AS2 diffusé par GS1 France pour plus d'informations techniques et fonctionnelles.

AS2FROM Ce terme contient une chaîne texte identifiant l'émetteur dans un échange de données.

AS2TO Ce terme contient une chaîne texte identifiant le destinataire de l'échange de données.

Cryptage Codage des données bloquant tout accès non autorisé, en particulier durant une transmission (sous AS2 par exemple) ou un stockage sur un média amovible magnétique. Le décodage nécessite une clé.

3DES Acronyme " Triple Data Encryption Standard". DES est une norme de cryptage très largement utilisée et reposant sur une algorithme complexe développé par le U.S. National Bureau of Standards.
3DES (prononcer triple-des) est une méthode de cryptage. 3DES implique 3 opérations cryptographiques DES, chacune étant opérée avec une clé de 56 bits différente. La longueur de clé 3DES s'élève à 168 bits. Voir la définition "DES".

EANCOM® Subsets des messages au standard EDIFACT adaptés au secteur de la distribution par EAN International.

EDI Acronyme "Electronic Data Interchange (Échange de Données Informatisé)". Transmission d'ordinateur à ordinateur, d'application à application, de données structurées selon des messages préétablis et normalisés via un moyen de télécommunication. Cette technique permet l'échange automatisé de données codifiées et agencées selon un langage préalablement convenu entre des applications logées sur des systèmes d'information distincts et hétérogènes. Les échanges sont effectués au moyen de différents réseaux de télécommunications.

EDIFACT Acronyme "Electronic Data Interchange for Administration, Commerce and Transport (Échange de Données Informatisé pour l'Administration, le Commerce et le Transport)". Règles des Nations unies concernant l'échange de données informatisé pour l'administration, le commerce et le transport. Elles se composent d'un ensemble de normes approuvées à l'échelon international, de répertoires et de directives pour l'échange électronique de données structurées, en particulier celles concernant le commerce des biens et services entre systèmes informatiques indépendants.

EEP Acronyme "Echanges Electroniques Professionnels" Les EEP peuvent se définir comme étant les activités nécessaires à l'échange d'information de système d'information à système d'information sans intervention humaine. Par extension, on étend la définition aux interfaces distantes avec un partenaire qui n'intègre pas les données directement dans son système d'information (WebEDI, EFI, Site marchand…).

EFI Acronyme "Échanges de Formulaires Informatisés". L'EFI, échange de formulaires informatisés, est une forme simplifiée de l'EDI qui permet à un utilisateur d'émettre ou de recevoir des documents électroniques structurés en mettant à sa disposition des grilles de lecture ou de saisie, simples, appelées formulaires. Cette application concerne les grands donneurs d'ordres dans leurs relations avec de petits ou moyens fournisseurs ou sous-traitants, l'Administration dans ses relations avec ses administrés, entreprises ou particuliers, ainsi que les PME et très petites entreprises dans leurs relations entre elles.

FTP Acronyme "File Transfer Protocol" Protocole de transfert de fichier. Par extension, il s'agit du nom de l'utilitaire, originellement disponible sous le système d'exploitation Unix, utilisant le protocole TCP/IP, pour télécharger des fichiers dans un sens ou dans l'autre (émission ou réception de données). D'une façon générique, il s'agit du nom des programmes offrant ce service.

GLN Acronyme "Global Location Number". Code lieu-fonction international EAN/UCC utilisant une structure à 13 chiffres. Un lieu-fonction désigne toute entreprise ou service d'une entreprise qui participe au titre d'une ou plusieurs fonctions à la réalisation d'une transaction commerciale.

GTIN Acronyme "Global Trade Item Number" (code article international EAN/UCC). Le GTIN peut être un des codes standards suivants : EAN/UCC-8, UCC-12, EAN/UCC-13 ou EAN/UCC-14.

HTTP / HTTPS Acronyme "Hyper Text Transfer Protocol/ Hyper Text Transfer Protocol Sécurisé".
C'est le protocole de communication utilisé pour accéder aux serveurs Web (WWW).

IP Acronyme de "Internet Protocol". Développé par le ministère de la Défense des Etats-Unis, IP est un protocole d'interconnexion de réseaux, de couche 3 dans le modèle référence OSI, qui assure le routage des données. Il fait partie du protocole de communication TCP/IP. Voir la définition "OSI" et "TCP-IP".

MD5 Acronyme "Message Digest 5 Algorithm". L'algorithme MD5 prend un message en entrée d'une longueur quelconque et en produit une signature "digitale" de 128 bits ("fingerprint" ou "message digest"). Il est supposé qu'il est informatiquement impossible de produire deux messages ayant la même signature. L'algorithme MD5 est destiné aux applications intégrant la signature électronique, où des fichiers volumineux doivent être compressés de façon sécurisée, avant d'être cryptés avec une clé privée (secrète) sous un système cryptographique à clé publique comme RSA.

OSI Acronyme de "Open Systems Interconnection". Architecture à sept niveaux qui standardise des niveaux de services et des types d'interaction lors d'échanges d'informations entre les ordinateurs d'un réseau. Elle est utilisée pour décrire le flux de données entre la connexion physique au réseau et l'application finale. Très répandu, ce modèle est largement utilisé pour décrire les environnements de réseau.

Protocole Un protocole est un système de règles et procédures régissant la communication entre plusieurs périphériques. Les protocoles ne sont pas toujours compatibles, mais deux périphériques utilisant le même protocole peuvent communiquer entre eux. Un protocole d'application fonctionne au niveau supérieur du modèle de référence OSI (voir définition OSI), fournissant l'interaction et l'échange de données entre applications. Les plus connus sont : SMTP (Simple Mail Transfer Protocol)-protocole TCP/IP de transfert de courrier électronique ; Telnet-protocole TCP/IP de connexion aux hôtes distants et de traitement local des données etc.
...

Réseau de communication Un réseau de communication est un système dans lequel sont reliés plusieurs ordinateurs indépendants afin de partager des données.

RVA Acronyme "Réseau à Valeur Ajoutée". Un RVA consiste en un réseau de télécommunication géré par un opérateur permettant de faire communiquer des applications et des matériels informatiques hétérogènes en apportant des fonctionnalités supplémentaires comme l'extraction, la traduction, le formatage ou le choix du protocole de communication.

SHA1 Acronyme de "Secure Hash Algorithm version 1". Il a été développé par la NIST (National Institute of Standards and Technology). La version actuelle date d'avril 1995. Il a les mêmes propriétés que MD5, mis à part qu'il produit des empreintes d'une longueur de 160 bits. Il est plus récent et réputé plus sûr que MD5.

S/MIME Acronyme "Secure/Multipurpose Internet Mail Extensions" C'est un format et un protocole dédiés à la signature cryptée et/ou à des services de cryptage pour des messages MIME (Multipurpose Internet

Mail Extensions = format conçu pour transférer par e-mail des données codées qui ne sont pas du texte par exemple images et autres fichiers binaires, etc.) transitant sur Internet.

SSCC Acronyme de "Serial Shipping Container Code" (numéro de colis). Identification unique d'une unité d'expédition utilisant une structure de codification standard à 18 chiffres.

TCP/IP Acronyme de "Transmission Control Protocol / Internet Protocol". Ensemble de protocoles qui permettent de communiquer à travers des réseaux locaux ou mondiaux interconnectés, faits d'ordinateurs et de systèmes d'exploitation très différents. TCP-IP comprend des standards qui définissent la manière dont communiquent les machines, ainsi que des accords pour connecter les réseaux et router le trafic. La plupart des réseaux acceptent TCP/IP.

Traducteur Ensemble logiciel utilisé pour convertir une information dans une codification et/ou selon un format donné dans une autre codification et/ou selon d'autres règles de formatage. (structuration). Le logiciel traduit les données d'un fichier interne préparé par une application interne, en données d'un langage commun (UN/EDIFACT : United Nations/ Electronic Data Interchange for Administration, Commerce and Transport = Échange de Données Informatisé pour l'Administration, le Commerce et le Transport), puis il génère la structure du message normalisé en mettant, au bon endroit dans la structure, les données traduites.

URI Acronyme de "Uniform Resource Identifier", terme générique pour les noms et les adresses se référant un objet du World Wide Web (WWW). Une URL ("Uniform Resource Locator") est une forme d'URI.

WEB EDI Outil permettant l'échange de données entre une communauté d'entreprises qui utilise des traitements d'échange automatisés et une communauté d'entreprises qui utilise des formulaires électroniques. Le Web EDI ou EDI formulaire est une solution EDI maintenue à distance et bâtie sur les standards EDI et Internet.

X.400 Ensemble des règles définies par le CCITT (Comité Consultatif Télégraphique et Téléphonique) pour les transferts de messages normalisés. Elles sont issues des travaux de l'ISO et du CCITT. La messagerie du type X.400 permet des échanges entre des systèmes hétérogènes.

XML Acronym "Extensible Markup Language". Sous-ensemble de SGML, XML est un méta langage qui permet de définir d'autres langages à partir de la création de balises auxquelles on donne une signification sémantique. XML permet à une entreprise de créer directement son propre vocabulaire et d'assembler les mots ainsi créés en messages. Dans XML, les DTD et/ou les schémas jouent le rôle de modèle pour cette création. Ces possibilités font d'XML un outil universel pour la conception, le transport, la transformation et l'exploitation des données textuelles et multi-média.

Zlib ZLIB (Z library) est un algorithme de compression ouvert, non-propriétaire et virtuellement portable sur tous les systèmes d'exploitation (écrit en langage de haut niveau, indépendant des matériels). Contrairement à la méthode de compression LZW, initialement utilisée sous Unix, et au format graphique GIF, la méthode de compression de ZLIB n'augmente jamais la taille des données (LZW peut doubler voire tripler la taille d'un fichier dans les cas extrêmes). La signature numérique de ZLIB est par ailleurs indépendante des données entrantes, et peut être réduite, si nécessaire, lors de la compression.

GS1 France

21 boulevard Haussmann
75009 Paris
T +33 (0)1 40 22 17 00

E info@gs1fr.org
www.gs1.fr