CONVENTION DE KYOTO

ANNEXE GENERALE

DIRECTIVES

Chapitre 7

APPLICATION DE LA TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION

ORGANISATION MONDIALE DES DOUANES

Version7 Mars 2014

« Copyright © 2014 World Customs Organization. Tous droits de traduction, de reproduction et d'adaptation réservés pour tous pays. Toute demande concernant la traduction, la reproduction ou l'adaptation du présent document doit être adressée à copyright@wcoomd.org ».

TABLE DE MATIERES

TABLE DE MATIERES 3
1. RECAPITULATIF 9
1.1 Objet des Directives 9
1.2 Le rôle stratégique de la TIC 9
1.3 Tendances futures 14
1.4 Portée 18
1.5 Table de concordance avec la Convention de Kyoto 19
2. AVANTAGES QUE PRESENTE LA TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION (TIC) 20
2.1 Introduction 20
2.2 Contrôles douaniers plus efficaces 20
2.3 Dédouanement plus efficace 21
2.4 Application uniforme de la législation douanière 22
2.5 Recouvrement plus efficace des recettes 22
2.6 Analyse plus efficace des données 22
2.7 Efficacité de l'établissement des statistiques du commerce extérieur 23
2.8 Meilleure qualité des données 23
3. LE PROCESSUS DE DECISION 24
3.1 Gestion du changement 24
3.1.1 Les dix étapes de la mise en œuvre du changement 25
3.1.2 Raisons pour lesquelles le changement échoue 28
3.1.3 Comment garantir le succès 29
3.2 A qui confier la conception du système ? 29
3.2.1 Choix d'un consultant 31
3.3 Comité directeur 31
3.4 Différents types de planification 32
3.4.1 Planification stratégique 32
3.4.2 Planification des projets 33
3.4.3 Planification de la continuité des activités 34
3.5 Elaboration d'une architecture d'entreprise : 36
4. IMPORTANCE DES CONSULTATIONS 39
4.1 Les entreprises 39

4.2 Les fonctionnaires des douanes ... 39
5. PROCESSUS DE MISE AU POINT DES SYSTEMES ... 41
5.1 Enquête détaillée et analyse du système existant ... 41
5.2 Conception détaillée du système ... 42
5.3 Programmation ... 43
5.4 Le processus d'acquisition ... 43
5.4.1 Acquisition ... 43
5.4.2 Appel d'offres ... 44
5.4.3 Evaluation des soumissions ... 45
5.4.4 Installation ... 46
5.5 Mise en oeuvre du système ... 47
5.5.1 Mise à l'essai du système ... 47
5.5.2 Conversion des fichiers ... 48
5.5.3 Formation des usagers ... 48
5.5.4 Stratégie du changement ... 49
5.6 Evaluation postérieure à la mise en œuvre ... 50
5.7 Entretien du système ... 51
5.7.1 Motifs de l'entretien ... 51
5.7.2 Types d'entretien ... 52
5.7.3 Responsabilité de l'entretien ... 52
5.8 Installation d'un Service d'Assistance ... 53
5.8.1 Engagement de service auprès des usagers de la douane ... 53
5.8.2 La douane a-t'elle besoin d'un service d'assistance? ... 54
5.8.3 Les différents aspects d'un Service d'Assistance ... 55
5.8.4 Le Service d'Assistance en tant que porteur de valeur ... 55
5.8.5 Comment mettre en place un Service d'Assistance? ... 57
5.8.6 Comment évaluer un Service d'Assistance ? ... 57
5.8.7 Incidence du Service d'Assistance sur le fonctionnement de la douane ... 58
6. APERCU DES PRINCIPAUX DOMAINES D'APPLICATION ... 59
6.1 Introduction ... 59
6.2 Validation des données ... 60
6.3 Contrôle d'inventaire des cargaisons ... 62
6.4 Traitement des déclarations de marchandises (à l'importation et à l'exportation), et notamment traitement avant l'arrivée/le départ des marchandises ... 63
6.4.1 Traitement avant l'arrivée/le départ des marchandises ... 64
6.4.2 Gestion des licences, permis, certificats et autres types d'autorisations ... 64

6.5 Rapprochement des renseignements ... 65
6.6 Notification de la mainlevée ... 65
6.7 Lutte contre la fraude douanière ... 65
6.8 Sélection ... 66
6.8.1 Gestion des risques ... 67
6.9 Contrôle préalable des voyageurs ... 67
6.10 Comptabilité des recettes ... 69
6.11 Statistiques du commerce extérieur ... 70
6.12 Systèmes intégrés de gestion (SIG) ... 70
6.13 Etablissement de rapports ... 71
6.14 Gestion du cycle de vie des données ... 71
6.14.1 Recherche des données ... 71
6.14.2 Exploration des données ... 71
6.15 Système d'enregistrement des opérateurs commerciaux ... 71
6.16 Transit douanier ... 72
6.17 Autres applications ... 73
6.18 Bureautique ... 73
6.19 Intranet et extranet en milieu douanier ... 74
7. EXTERNALISATION DES FONCTIONS DOUANIERES ... 75
7.1 Aperçu ... 75
7.1.1 Externalisation, délocalisation et internalisation ... 75
7.1.2 Croissance de l'externalisation ... 75
7.2 Externalisation au sein de la douane et domaines pouvant être externalisés : activités essentielles et activités non essentielles ... 76
7.3 Avantages de l'externalisation ... 77
7.3.1 Retour aux activités essentielles ... 77
7.3.2 Responsabilité ... 77
7.3.3 Qualité ... 77
7.4 Enjeux de l'externalisation ... 77
7.4.1 Questions liées à la qualité des services ... 77
7.4.2 Questions liées aux ressources humaines ... 78
7.4.3 Questions liées à la sécurité ... 78
7.5 Conclusion : comment établir l'équilibre approprié ... 79
8. INTERFACES ENTRE APPLICATIONS DE TI ... 80
8.1 Architecture orientée services ... 81
9. ECHANGE DE RENSEIGNEMENTS ... 84

9.1 Echanges de renseignements avec les opérateurs commerciaux 84
9.2 Echanges de renseignements avec d'autres administrations 85
9.3 Echanges de renseignements avec d'autres administrations des douanes 86
10. COMMUNICATIONS 88
10.1 Solutions en matière de transmission des données 88
10.2 Télécommunications 89
10.3 Conception des messages 89
11. SECURITE EN MATIERE DE TIC 92
11.1 Sécurité en matière de TIC – Définition et objectif 93
11.2 Politique en matière de sécurité de la TIC 93
11.3 Sécurité de la TIC – Aspects à prendre en compte 94
11.4 Authentification 98
11.4.1 Pourquoi l'authentification est-elle nécessaire ? 98
11.4.2 Variantes électroniques 99
11.4.3 Quelle méthode utiliser ? 104
11.4.4 Risques acceptables 105
11.4.5 Comparaison des méthodes d'authentification 106
11.5 Non-répudiation 106
11.5.1 Définition de la non-répudiation 107
11.5.2 La non-répudiation n'est pas une question isolée 107
11.5.3 Incidence de la répudiation sur le plan juridique 108
11.5.4 Assurance 109
11.5.5 Motifs de la répudiation 109
11.6 Assurance de l'identité 110
11.6.1 Preuve de l'identité 110
11.6.2 Preuve de l'autorisation 111
11.6.3 Le cadre 111
11.7 Assurance du contenu 111
11.7.1 Assurance de l'intégrité 111
11.7.2 Rassembler les différentes parties 112
11.7.3 Stockage et reproduction 112
11.8 Intégrité des processus 112
11.8.1 Cadre de gestion 112
11.8.2 Architecture et règles du système 112
11.9 Infrastructure à clé publique (ICP) 113
11.9.1 Données générales 113

11.9.2 Définition de l'ICP ... 113
11.9.3 Comparaison entre une signature conventionnelle et une signature numérique ... 114
11.9.4 Durée de vie utile d'un certificat numérique ... 114
11.9.5 Considérations importantes liées à la mise en œuvre de solutions reposant sur l'ICP 115
11.9.6 Utilisation des signatures numériques dans les messages EDI et XML ... 116
11.9.7 Autorité de certification et cadre légal ... 116
11.9.8 L'ICP et la douane : principales questions à examiner ... 117
11.9.9 Gestion de l'identité ... 118
12. QUESTIONS JURIDIQUES ... 122
12.1 Introduction ... 122
12.2 La législation en vigueur est-elle adéquate ? ... 122
12.3 Types de questions juridiques ... 122
12.4 Signature ... 123
12.5 Recevabilité ... 124
12.6 Protection des données et protection de la vie privée ... 124
13. AUDITS DES CONTROLES INTERNES DES SYSTEMES INFORMATIQUES ... 126
13.1 Généralités ... 126
13.2 Audits de conception ... 126
13.3 Planification ... 127
13.4 Enquête ou recueil de renseignements ... 128
13.4.1 Entretiens ... 128
13.4.2 Examen de la documentation ... 128
13.5 Consignation des résultats d'un audit ... 129
13.6 Evaluation ... 129
13.7 Confirmation des conclusions d'un audit ... 129
13.8 Rapport ... 130
13.9 Vérification après audit ... 130
13.10 Conclusion ... 130
14. PROBLEMES COURANTS ... 131
14.1 Introduction ... 131
14.2 Résistance culturelle ... 131
14.3 Informatisation des données de base ... 131
14.4 Absence d'infrastructure adéquate ... 132
14.5 Législation douanière ... 132
14.6 Limitation des ressources et des compétences ... 132

APPENDICE 1 - STRUCTURES DE L'INFORMATION ET DES TELECOMMUNICATIONS POUR LE COMMERCE ELECTRONIQUE 133

APPENDICE 2 - STRUCTURES DE L'INFORMATION ET DES TELECOMMUNICATIONS POUR LE COMMERCE ELECTRONIQUE 140

APPENDICE 3 - PROCEDE DE SELECTION LOCAL 141

APPENDICE 4- SYSTEME DE FILTRE DES PROFILS DE SELECTION 142

APPENDICE 5 - MODÈLE DE PROCÉDURES DOUANIÈRES ET D'EXPLOITATION DES FICHIERS 144

APPENDICE 6 - DIAGRAMME DE TRAITEMENT PAR ORDINATEUR 146

APPENDICE 7 – Glossaire des termes et abréviations 147

Appendice 8 - DIAGRAMME FONCTIONNEL DE LA TECHNOLOGIE DE L'INFORMATION155

Appendice 9 – Recommandation de l'OMD concernant la TI 157

Appendice 10 – Recommandation de l'OMD relative à l'utilisation des sites Web par les administrations des douanes 159

Appendice 11 – Recommandation de l'OMD relative au Guide de l'OMD régissant la répartition des données 165

Appendice 12 – Recommandation de l'OMD relative aux données exigées aux fins des RPCV 167

Appendice 13 – Recommandation de l'OMD concernant l'utilisation de l'UNTDED 169

Appendice 14 – Recommandation de l'OMD concernant les règles de syntaxe EDIFACT 171

Appendice 15 – Recommandation de l'OMD relative à l'utilisation de codes pour les éléments de données 174

Appendice 16 – Recommandation de l'OMD concernant les renseignements douaniers traités par ordinateur 185

Appendice 17 – Recommandation de l'OMD concernant l'utilisation des normes CCD/IATA 187

Appendice 18- RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'UTILISATION DU MODELE DE DONNEES DE L'OMD 189

Appendice 19 RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'EMPLOI DES RENSEIGNEMENTS PREALABLES CONCERNANT LES VOYAGEURS (RPCV) ET DES DOSSIERS PASSAGERS (PNR) 191

AFIN D'ASSURER L'EFFICACITE DES CONTROLES DOUANIERS 191

1. RECAPITULATIF

1.1 Objet des Directives

Les présentes Directives ont pour objet d'appeler l'attention des administrations des douanes sur l'incidence des technologies de l'information et de la communication (IC ou "TIC" mais parfois également appelées "TI") sur les activités douanières. Elles décrivent comment la douane peut utiliser cette technique pour améliorer la réalisation de ses programmes et planifier les améliorations à apporter aux services qu'elle offre à ses clients et à ses partenaires commerciaux. Elles ne sont pas destinées à fournir un catalogue des dernières technologies disponibles ou à suggérer des solutions dans le domaine du matériel et/ou des logiciels. Elles s'attachent avant tout aux grands principes régissant l'usage de la TIC dans les administrations douanières.

1.2 Le rôle stratégique de la TIC

Les autorités publiques du monde entier sont aujourd'hui tenues de dispenser des services publics part voie électronique. Pour la douane, cet impératif s'est imposé plus tôt que pour les autres administrations. Il était normal que la douane, compte tenu de ses responsabilités importantes en matière de contrôle des marchandises, de perception des recettes et de surveillance des frontières, utilise dans un premier temps des systèmes informatiques pour contrôler l'inspection et la vérification des marchandises, ainsi que la perception des recettes connexes.

Les administrations des douanes ont ensuite commencé à utiliser la TIC pour passer de l'inspection des marchandises à celle des renseignements pertinents figurant sur les déclarations à l'importation et à l'exportation établies sur papier. Elles ont constaté qu'elles pouvaient également réduire l'obligation pour les entreprises de présenter de nombreux exemplaires de documents "originaux" sur papier puisque les principaux renseignements étaient saisis par un système informatique qui pouvait non seulement valider et traiter les données, mais également les stocker à un coût très inférieur à celui du stockage de dossiers sur papier.

Toutefois, en l'état alors rudimentaire de la TIC, la douane avait toujours besoin que les documents lui soient présentés matériellement par le déclarant ou par ses représentants en un lieu et à un moment qui lui convenaient et qu'elle spécifiait elle-même. Par la suite, les évolutions de la TI ont offert la possibilité de communiquer de manière instantanée et directe. Ces technologies ont transformé les structures et les règles de procédure courantes. Par exemple, la douane peut séparer la mainlevée du dédouanement. Les renseignements électroniques, reçus bien avant l'arrivée des marchandises, permettent à la douane de disposer de toutes les informations nécessaires aux fins des contrôles.

Les organisations douanières modernes sont très dépendantes de l'application de la TIC. L' exigence par les parties concernées d'une amélioration de l'efficacité en matière de facilitation des échanges et d'un respect de la loi continue d'inciter les dirigeants de la douane à investir dans des projets et des initiatives basés sur la TI. Les systèmes avancés

de gestion du risque et de Guichet unique nécessitent l'emploi de technologies sophistiquées et obligent à des investissements complexes et massifs en matériel, en logiciel et en services.

Dans un certain nombre d'administrations des douanes, les systèmes hérités de périodes antérieures continuent d'être employés et ce, pour diverses raisons. Même si certains de ces systèmes ne bénéficient plus d'aucune assistance de la part des vendeurs, les administrations sont obligées de continuer et de les maintenir en bon état afin de préserver un niveau satisfaisant de performance en matière de facilitation des échanges.

Selon certaines estimations, dans les principales entreprises du secteur des services, le coût d'exploitation de la technologie de l'information représente le second poste de dépenses après celui des ressources humaines et mobilise 5 à 7 % du total des frais d'exploitation. (Source : Gartner Consulting – Worldwide IT Benchmark Services)

La TIC a longtemps été considérée comme un service de soutien ou d'accompagnement. Ce point de vue a récemment évolué et la TIC est à présent reconnue comme un élément moteur des transformations et comme un moyen de bénéficier d'un avantage concurrentiel.

Les dirigeants doivent comprendre les processus à travers lesquels la TI crée de la valeur pour l'organisation. Il est nécessaire à cet égard d'adopter des cadres de gouvernance apportant clarté et transparence, en expliquant aux parties concernées quel est le lien entre les résultats obtenus et les investissements consentis pour la TI. Les réalisations dues à la TIC doivent être expliquées en termes opérationnels.

C'est dans ce contexte que s'est développée la nouvelle discipline de Gouvernance de la Technologie de l'information, reposant essentiellement sur les principes de responsabilité des dirigeants et de contrôle stratégique, auxquels s'ajoutent un certain nombre de structures et de compétences professionnelles qui répondent aux besoins des dirigeants au niveau administratif comme au niveau des responsables opérationnels.

La question des processus décisionnels liés à la TI, envisagée comme une question stratégique au sein de l'organisation, a été incluse aux Directives. Il convient de décrire la méthode que les administrations douanières doivent mettre en place pour lier les objectifs stratégiques de l'organisation avec les processus de TI concernés.

Ce travail aidera la douane à asseoir ses missions de renforcement des capacités sur les processus de TI les plus importants. C'est également dans cette partie que doit être abordée la question de la pertinence de l'Architecture d'entreprise dans la gestion des investissements stratégiques destinés à la TI.

Toute administration douanière a pour objectif de préserver la valeur dans la chaîne logistique internationale en améliorant l'efficacité des contrôles transfrontières de manière à ne pas interrompre le flux des marchandises, à préserver la sécurité des frontières et à empêcher toute fuite des recettes fiscales. Les responsables de la douane et des entreprises appréhendent cette valeur en termes d'efficacité des contrôles et d'efficience de la chaîne logistique. La TIC doit contribuer à ces efforts et la douane comme les entreprises doivent atteindre les objectifs opérationnels en s'appuyant sur les capacités sans cesse renouvelées de la TIC.

Les investissements en TI ont considérablement augmenté durant la dernière décennie mais la perception du retour sur investissement n'est pas uniforme. Il n'est pas rare de voir des dirigeants développer une attitude critique vis-à-vis des travaux accomplis au sein de l'organisation en matière de TI et faire preuve de peu d'entrain pour les résultats obtenus. D'autres responsables, qui comprennent la valeur générale de l'investissement proposé, ne sont pas en mesure d'établir un lien entre ces investissements et les résultats obtenus. Il est nécessaire de disposer d'une structure aidant les dirigeants à surveiller la valeur réellement ajoutée par les investissements en matière de TIC et permettant d'avoir une garantie crédible que les objectifs de l'organisation sont conformes à ceux des projets et services de la Technologie de l'information. Le COBIT est un outil majeur de gouvernance et de contrôle des TI qui sépare l'ensemble du champ de la gouvernance en matière de TI en "Objectifs de contrôle", tels que répertoriés ci-après.

Planifier et organiser

PO1: Définir un plan informatique stratégique.

PO2: Définir l'architecture de l'information.

PO3: Déterminer l'orientation technologique.

PO4: Définir les processus, l'organisation et les relations de travail.

PO5: Gérer les investissements informatiques.

PO6: Faire connaître les buts et les orientations du management.

PO7: Gérer les ressources humaines de l'informatique.

PO8: Gérer la qualité.

PO9: Évaluer et gérer les risques.

PO10: Gérer les projets.

Acquérir et implémenter

AI1: Trouver des solutions informatiques.

AI2: Acquérir des applications et en assurer la maintenance.

AI3: Acquérir l'infrastructure technique et en assurer la maintenance.

AI4: Faciliter le fonctionnement et l'utilisation.

AI5: Acquérir des ressources informatiques.

AI6: Gérer les changements.

AI7: Installer et valider des solutions et des modifications.

Délivrer et supporter

DS1: Définir et gérer les niveaux de service.

DS2: Gérer les services tiers.

DS3: Gérer la performance et la capacité.

DS4: Assurer un service continu.

DS5: Assurer la sécurité des systèmes.

DS6: Identifier et imputer les coûts.

DS7: Instruire et former les utilisateurs.

DS8: Gérer le service d'assistance client et les incidents.

DS9: Gérer la configuration.

DS10: Gérer les problèmes.

DS11: Gérer les données.

DS12: Gérer l'environnement physique.

DS13: Gérer l'exploitation

Surveiller et évaluer

ME1: Surveiller et évaluer la performance des SI.

ME2: Surveiller et évaluer le contrôle interne.

ME3: S'assurer de la conformité réglementaire.

ME4: Mettre en place la gouvernance des SI.

Ce Cadre s'accompagne d'un ensemble d'outils grâce auxquels les responsables peuvent prendre en compte les exigences liées aux contrôles, les questions techniques et les risques opérationnels. Il offre un traitement complet de la gouvernance de la TI et couvre un vaste éventail de questions qu'un responsable de la douane se doit de contrôler. Les Directives sur la TIC abordent la plupart de ces questions dans différentes sections.

- pour améliorer la perception des recettes et la gestion de la politique commerciale à l'importation et à l'exportation ;

- pour accélérer la mainlevée des envois à l'exportation et à l'importation et offrir d'autres procédures préférentielles aux clients qu'elles considèrent comme étant les plus fiables en matière de respect de la loi et comme présentant donc moins de risques à l'égard de la perception des recettes et autres responsabilités douanières;

- pour répondre aux préoccupations du gouvernement et des usagers qui souhaitent que les marchandises prohibées, les espèces menacées d'extinction, les droits de propriété intellectuelle, etc. fassent l'objet de contrôles efficaces ; et

- pour assurer l'intégrité et l'efficacité de la gestion du mouvement des marchandises et des voyageurs.

Les administrations des douanes modernes doivent faire face à l'échelon international à toute une série d'innovations commerciales diverses reposant sur des applications de TI, notamment des services de transport par express et autres services globaux par transport multimodal, et un réseau croissant de systèmes mondiaux d'approvisionnement, de production et de distribution alimentés par des réseaux logistiques de gestion à flux tendu.

Veiller à ce que les pratiques utilisées par la douane demeurent au diapason de ces développements commerciaux appellera des changements tout aussi novateurs dans les principes de base de la gestion administrative.

Alors que de nombreuses administrations utilisent ou envisagent d'utiliser les TIC pour améliorer leurs opérations, la plupart des procédures actuellement employées par la douane reposent toujours sur la réception d'équivalents électroniques des anciens documents échangés. Les déclarations sur papier ont simplement été remplacées par des messages EDI.

Les administrations qui envisagent actuellement de concevoir ou d'améliorer leurs applications d'IC devraient franchir un nouveau pas en constatant que pratiquement toutes les données dont la douane a besoin existent déjà dans les systèmes d'information commerciale utilisés pour effectuer les transactions commerciales.

Elles devraient déterminer dans quelle mesure leurs propres besoins en données de contrôle peuvent être remplis par les systèmes d'information de leurs partenaires commerciaux après qu'ils aient fait l'objet d'un audit pour s'assurer qu'ils sont sûrs, qu'ils sont capables de reproduire les données avec précision et possèdent des facilités appropriées en matière de conservation et d'archivage des données.

Si, comme c'est généralement le cas aujourd'hui, ces systèmes de TI s'avèrent fournir des données plus précises et plus facilement exploitables à des fins douanières que les échanges de documents traditionnels sur papier, les administrations des douanes seront de plus en plus en mesure de se fier aux systèmes informatisés de leurs partenaires commerciaux agréés qui auront fait l'objet d'un contrôle pour répondre à leurs propres besoins en matière de données de nature fiscale, commerciale et autre.

La plupart des administrations des douanes sont aujourd'hui obligées de supporter une charge de travail croissante liée au contrôle des marchandises et des voyageurs, et ce avec les effectifs existants, et même parfois réduits. Nombre d'entre elles ont déjà démontré que le recours aux TIC a amélioré la qualité de la saisie et de la gestion des informations et qu'il a permis de libérer des ressources peu nombreuses afin de les concentrer sur les principales tâches de lutte contre la fraude, notamment l'identification et le contrôle des personnes et des envois suspects.

Les présentes Directives recommandent aux administrations des douanes qui utilisent les TIC de respecter les normes internationales pertinentes. Il est indispensable que toute norme réellement employée dans les applications informatiques soit aisément identifiable et disponible aux fins de tout échange nécessaire avec les autres administrations.

Avant d'adopter une application en matière d'IC, les administrations doivent consulter les parties intéressées susceptibles d'être touchées, notamment les autres services publics ainsi que les entreprises, les transporteurs, les agents, les exploitants de ports et d'aéroports, afin de s'assurer que toutes pourront aisément appliquer la solution retenue. Un mécanisme permanent de consultation avec ces partenaires, à tous les stades ultérieurs de la conception du système, leur permettra de concevoir et d'adapter leurs propres systèmes, et les encouragera à le faire, afin d'utiliser au mieux les innovations de la douane et d'en offrir également la meilleure utilisation possible.

Les présentes Directives ont certes pour principal objet d'appeler l'attention de l'ensemble des administrations des douanes sur l'utilisation des TIC dans le cadre de leurs propres opérations, mais les administrations devront suivre, et en tenir pleinement compte, les applications parallèles pertinentes, liées à l'évolution rapide des pratiques commerciales, qui ont eu, et continueront d'avoir, de profondes répercussions sur la gestion quotidienne.

1.3 Tendances futures

Alors que, par le passé, l'OMD a essentiellement étudié l'utilisation des TIC dans le cadre d'opérations douanières conventionnelles, les échanges de vues tenus récemment ont commencé à examiner leur incidence sur l'ensemble des fonctions de la douane.

Il est aujourd'hui évident que la douane devra abandonner la notion de «taille unique», et passer à une philosophie de systèmes ouverts qui lui permettra d'échanger des informations, par différents moyens électroniques avec des employés, des clients appartenant ou non aux milieux commerciaux et, à l'échelon national et international, avec d'autres services et organes officiels compétents.

Lorsqu'elle planifiera cette transformation, la douane devra tenir compte du fait qu'entre un tiers et la moitié de l'ensemble des échanges internationaux consistent aujourd'hui en transactions, inter-entreprises dans lesquelles des matériaux, des composants et des produits finis et/ou semi-finis franchissent les frontières nationales dans le cadre de systèmes de gestion commerciale intégrés, et ce dans des délais de plus en plus courts et de plus en plus exigeants.

Les autres secteurs commerciaux, qui participent à des opérations traditionnelles de vente et d'achat, demandent les conseils et l'aide de prestataires de services logistiques pour simuler ces systèmes très efficaces de gestion ininterrompue des transactions.

Dans tous les pays, la douane continue de traiter ces mouvements comme une série d'opérations d'exportation ou d'importation distinctes. Chaque administration ne voit et ne traite que la moitié de chaque transaction internationale.

Pour pouvoir améliorer considérablement les contrôles douaniers, en faisant face de manière très novatrice à des pratiques commerciales maintenant bien établies et dont l'utilisation se répand rapidement, il est indispensable d'élaborer et de mettre en oeuvre, aux

fins de l'assistance mutuelle entre administrations douanières, des accords bilatéraux et multilatéraux qui permettront de gérer de manière uniforme tout un jeu de contrôles et de procédures.

Plusieurs administrations des douanes ont lancé des projets pilotes et prototypes en coopération avec certaines entreprises intéressées en vue d'étudier et de mettre à l'essai les jeux de données et les normes de communication nécessaires, de définir les obstacles de nature juridique et d'évaluer les coûts/avantages pratiques qu'en tireraient tous les participants.

L'expérience acquise à ce jour dans le cadre de ces projets a révélé que, même si les technologies nécessaires existent déjà, les cadres juridiques qui régissent actuellement la circulation des marchandises et des informations à l'échelon international et national devront être examinés et éventuellement modifiés.

Les techniques de gestion à flux tendu ont inévitablement entraîné la multiplication des petits envois, répétitifs et fréquents. Dans la mesure où, à des fins douanières, chaque envoi doit être assorti de son propre jeu de données de contrôle, cela aurait pu soulever de graves problèmes de traitement de l'information.

Fort heureusement, des transporteurs spécialisés utilisent déjà les TIC pour maximiser l'efficacité logistique, et ce dans tous les modes de transport ; la douane, en utilisant les systèmes de commerce électronique (CE) appropriés et une gamme toujours plus vaste de techniques d'échange de données informatisé (EDI), peut tirer parti de ces systèmes de circulation des données bien gérés pour alimenter ses propres procédures d'évaluation des risques et de mainlevée. De nombreux services douaniers ont adopté, ou mettront en œuvre des applications EDI au moyen de formats de messages normalisés, et principalement ceux de l'ONU/EDIFACT. Afin de garantir la compatibilité de ces messages, il est recommandé de développer tous les systèmes EDIFACT sur la base des cartes EDIFACT du Modèle de données de l'OMD.

Les normes EDIFACT/ONU qui définissent les structures des données pour pratiquement tous les types d'activités et documents officiels utilisés dans le cadre du commerce international sont toujours les seules à faire autorité à l'échelon mondial. Le langage de balisage extensible (Extensible Mark-up Language ou XML) s'est également imposé comme norme dominante. Les structures de données et les vocabulaires XML sont enrichis par différents organes de normalisation, dont l'OMD. Les nouvelles technologies et infrastructures de télécommunications comme celles offertes par Internet constituent pour la douane un moyen peu onéreux de recevoir et de diffuser des informations, notamment l'XML, l'édition de base de données, l'édition de documents et les formulaires électroniques. Un mécanisme approprié de consultation avec ses partenaires commerciaux permettra à la douane d'offrir à ses clients des milieux commerciaux diverses possibilités en matière d'échange d'informations; certaines d'entre elles sont décrites à l'Appendice

L'évolution rapide des technologies modèle le fonctionnement actuel des entreprises, et les prestations traditionnelles de services par voie électronique sont délaissées. En fonction de ses priorités stratégiques, chaque administration des douanes met l'accent différemment sur la nécessité de rester au contact des évolutions technologiques et toute utilisation nouvelle de la TI est justifiée par une situation particulière.

Plusieurs évolutions majeures de la TI apparaissent simultanément et elles vont changer le mode de prestation des services dans les années à venir. Certaines d'entre elles sont mentionnées ci-après :

1. Les dispositifs portables d'utilisateur final : les utilisateurs finals sont mieux équipés d'un point de vue technologique et ils ont aujourd'hui accès à des dispositifs bons marchés plus puissants que ne l'étaient les ordinateurs il y a quelques années seulement. Ces dispositifs se présentent sous des formes et des tailles différentes afin de répondre aux besoins particuliers de chaque utilisateur. Les téléphones intelligents et les tablettes constituent deux grandes catégories de dispositifs de ce type et les tablettes peuvent parfois être transformées en ordinateurs de bureau.

2. Internet depuis n'importe quel endroit : les dispositifs mobiles sont à présent connectés au réseau Internet sans fil et peuvent être en permanence « en ligne ». L'accès Internet à débit rapide sur les dispositifs mobiles et une réalité dans les pays industrialisés mais les pays moins développés sont également en train de combler leur retard. Les gouvernements peuvent ainsi améliorer l'accès à leurs applications par le biais d'Internet.

3. Les applications (APP) sont des logiciels d'un nouveau type qui fonctionnent sur les dispositifs portables (APP est une abréviation pour les applications logicielles). Les APP sont faciles à trouver, à acheter, à installer, à lancer, à faire fonctionner et à mettre à jour. La rapidité avec laquelle un consommateur peut accéder à des APP et les utiliser est inédite. Leur utilité et leur facilité d'utilisation représentent une avancée considérable. L'apport de nouvelles APP utiles et innovantes pour les dispositifs portables se renouvelle sans cesse et répond à toutes les principales fonctions commerciales. Les renseignements fournis par certains Membres de l'OMD donnent à penser que l'arrivée d'applications de ce type pour les entreprises n'est qu'une question de temps. On peut ainsi imaginer que les administrations douanières seraient en mesure d'offrir à l'utilisateur final la possibilité de disposer instantanément de solutions opérationnelles.

4. L'interface utilisateur : le clavier, la souris et l'interface utilisateur graphique sont concurrencés par l'interface tactile des dispositifs mobiles. Cette interface contraint les concepteurs de logiciels de définir comment il convient de convertir les fonctions opérationnelles en quelques mouvements du doigt sur une tablette. En d'autres termes, les développeurs s'efforcent de trouver des applications qui soient aussi commodes que possible pour l'utilisateur d'un dispositif portable. Ainsi, les obstacles découlant de l'utilisation de l'application sont moindres pour l'utilisateur. Par exemple, à moins de ne pas avoir d'autre choix, l'utilisateur ne sera pas tenu d'introduire de données, ce qui entraîne un niveau élevé de réutilisation des données opérationnelles.

5. Capacité de contextualisation et de géolocalisation des applications : des dispositifs intelligents ont à présent été élaborés et sont capables de révéler en temps réel le lieu où se trouvent les conteneurs, les marchandises, les moyens de transport, les employés de la logistique, les fonctionnaires des douanes et d'autres acteurs. Ces capacités offrent de nouvelles possibilités pour concevoir des applications de manière à ce que les flux d'informations et de marchandises se déplacent toujours ensemble. Les données obtenues à partir de dispositifs appelés des capteurs sont également appelées à jouer un grand rôle. Les capteurs utilisés pour suivre les conteneurs à la trace et les dispositifs d'identification par

fréquence radio (RFID) installés sur des scellements électroniques généreront les flux continus de données opérationnelles utiles.

6. Les médias sociaux se présentent sous la forme d'un ensemble d'applications sur Internet permettant la création et le partage d'informations par des utilisateurs qui font parti d'une communauté virtuelle. Les médias sociaux ont considérablement modifié la manière dont les organisations, les communautés et les personnes communiquent. Ils sont rapidement adoptés par les entreprises en tant que moyen de communication avec leurs clients et avec les parties concernées. Ils offrent aux administrations des douanes la possibilité de parvenir à une transparence et une cohérence des contrôles.

7. Gros volume de données (« Big data ») : les dispositifs intelligents, les réseaux sociaux et les unités de recueil de données des capteurs sont connectés aux systèmes d'entreprises, lesquels reçoivent en continu des volumes importants de données. Les technologies nécessaires pour gérer de tels volumes de données sont les technologies « big data », qui peuvent se révéler utiles pour les administrations douanières en générant des renseignements opérationnels précieux ou en contribuant à améliorer la gestion des risques.

8. Plate forme d'informatique en nuage ('cloud computing') : l'informatique en nuage est devenue plus importante dans le domaine de l'informatique d'entreprise. La technologie d'informatique en nuage contribue au conditionnement et à la présentation de ressources informatiques proposées à la consommation comme des serveurs ou des capacités de stockage et de mise en réseau et ce, à travers la notion de virtualisation sous la forme d'Infrastructures en tant que service. L'informatique en nuage couvre également des approches telles que les Logiciels en tant que service et les Plateformes en tant que service. La technologie d'informatique en nuage a rendu les ressources informatiques plus accessibles et plus rentables que les solutions traditionnelles. L'adoption des technologies d'informatique en nuages s'impose parmi les gouvernements, où elles sont souvent déployées sous la forme d'un « nuage privé ». Les risques liés à la sécurité des données sont ainsi moins importants puisque les données résident dans des centres de données que le gouvernement gère ou fait fonctionner. Les administrations trouvent ces solutions attirantes pour les raisons suivantes :

a. La technologie d'informatique en nuage contribue à éviter des dépenses en capital, et donc à réduire les risques liés aux investissements.
b. Tout en réduisant les coûts du lancement de projets pilotes et de démonstrations de faisabilité, elle aide à tester et lancer plus vite de nouvelles initiatives.
c. Dès qu'une application est prête pour la production, il devient facile d'accéder à l'infrastructure d'informatique en nuage qui peut assurer immédiatement la production.
d. L'informatique en nuage permet aux administrations de regrouper les ressources informatiques, et de profiter ainsi de la technologie tout en réglant au sein du gouvernement les questions de sécurité et de compétences sur les données.
e. Grâce à l'informatique en nuage, les administrations des douanes peuvent espérer externaliser les services informatiques « à la demande », sans s'impliquer dans l'achat et le fonctionnement de leurs propres infrastructures.
f. Certains services peuvent être utilisés de manière stratégique par le gouvernement plutôt que par des départements distincts faisant appel à de nombreuses parties tierces.

Il convient toutefois de souligner que l'emploi de l'informatique en nuage n'en est encore qu'à ses balbutiements et que cette technologie suscite d'importantes préoccupations en matière de sécurité. Les gouvernements souhaitent généralement savoir où se trouvent les données et veulent être en mesure de vérifier complètement l'accès et la confidentialité desdites données. Les gouvernements de tous les pays mettent donc en place des politiques formelles concernant l'informatique en nuage, et ce pour faire face aux enjeux que soulève cette technologie tout en tirant partie de son déploiement. L'informatique en nuage devrait être de plus en plus largement mise en oeuvre dans le cadre de projets entièrement nouveaux et aux fins d'applications non essentielles à une mission.

Dans le monde entier, les gouvernements mettent en place des politiques officielles d'informatique en nuage et l'on estime que cette technologie sera de plus en plus déployée pour des projets nouveaux et pour des applications qui ne sont pas essentielles dans une mission donnée.

Compte tenu de ces tendances futures, la douane devrait prévoir de modifier son infrastructure en matière de TIC.

1.4 Portée

Les présentes Directives ont été élaborées pour aider la douane à décider comment utiliser les TIC pour améliorer les services qu'elle offre à ses clients et partenaires commerciaux. Elles déterminent les principaux domaines des programmes offerts par la douane dans lesquels l'application des TIC s'avérera sans doute la plus bénéfique. Elles proposent et décrivent les éventuelles interfaces des partenaires commerciaux, ainsi que plusieurs facteurs dont les administrations doivent tenir compte aux fins de l'utilisation des TIC. Ces facteurs sont notamment les besoins et les questions d'ordre juridique, les aspects sécuritaires et la consultation des clients.

Les TIC permettent à la douane d'améliorer ses contrôles tout en renforçant parallèlement la facilitation. Pour tirer parti au maximum de ces avantages, une administration des douanes qui envisage d'appliquer les TIC devra au préalable étudier les procédures qu'elle applique pour dispenser ses programmes, en tenant compte du fait que la TIC ne peut qu'offrir des outils à l'appui d'activités de fond. Il est supposé que les procédures auront déjà été remaniées conformément aux normes, annexes et directives de la Convention de Kyoto révisée.

Les présentes Directives ne couvrent pas les solutions liées au matériel et/ou aux logiciels car elles doivent être choisies individuellement par chaque administration compte tenu de ses propres besoins et des besoins connexes de ses partenaires commerciaux.

Les présentes Directives visent :

- à encourager les administrations des douanes à effectuer des recherches et à utiliser les solutions offertes par les TIC à l'appui des contrôles et des procédures qu'elles appliquent actuellement;
- à conseiller et à inciter les administrations des douanes qui envisagent d'utiliser l'informatisation à respecter un processus/plan prédéfini couvrant tous leurs besoins;

- à promouvoir l'emploi de normes internationales dans les échanges de données électroniques entre les administrations des douanes et leurs partenaires commerciaux; et
- à conseiller les administrations des douanes au sujet des faits nouveaux actuels et futurs qui pourraient améliorer l'informatisation de la douane.

1.5 Table de concordance avec la Convention de Kyoto

Disposition de l'Annexe générale	**Partie des Directives relatives à la TI**
3.11	8, 9.3, 9.4
3.18	6.4
3.21	6.4
6.9	2, 6.6, 12
6.10	4

2. AVANTAGES QUE PRESENTE LA TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

(Norme transitoire 6.9, Normes 7.1 et 7.3)

2.1 Introduction

Cette partie décrit les principaux domaines dans lesquels la mise en place des TIC par la douane présente des avantages tant pour la douane elle-même que pour ses partenaires commerciaux, en tenant compte du fait que cette mesure peut avoir une incidence majeure sur les relations de travail entre la douane et les entreprises et que nombre des avantages que la douane peut tirer de l'introduction des TIC doivent être pleinement compris par les milieux commerciaux et appelleront d'ailleurs leur coopération.

La planification et la conception de l'informatisation devraient être assorties d'une analyse de rentabilité détaillée effectuée au préalable en consultation avec les milieux commerciaux intéressés afin de s'assurer que les solutions envisagées seront utiles et efficaces pour toutes les parties concernées. Il convient de rappeler que la mise en place de certaines technologies, par exemple l'EDI, par la douane oblige parfois les entreprises à investir des ressources dans la conception de logiciels d'interface nécessaires à leurs propres systèmes, outre les dépenses supplémentaires connexes liées par exemple aux frais du trafic de réseau.

La participation de représentants des entreprises, chaque fois que possible, au processus douanier de planification et de prise de décisions peut prendre diverses formes, mais les mesures les plus fréquemment prises consistent à créer un groupe consultatif douane/entreprises, appuyé par des réunions publiques, des dossiers et des bulletins d'information. Ce groupe consultatif est très important car il peut permettre aux parties extérieures à la douane qui sont directement touchées par le système proposé d'exercer une influence sur sa mise en oeuvre et de s'approprier les résultats ultérieurs. Ce groupe doit être créé au tout début du processus de planification du projet et se réunir régulièrement pendant toute sa durée de vie.

La tenue de réunions publiques, ouvertes à toutes les entreprises individuelles, ainsi qu'à leurs représentants, constitue un moyen utile de transmettre des informations à un large public commercial, et d'en recevoir en contrepartie. Ces réunions doivent être appuyées par la mise à disposition de dossiers d'information décrivant le système proposé et la manière dont il pourrait affecter et modifier les opérations commerciales, avec des précisions concernant les exigences des systèmes de l'entreprise.

2.2 Contrôles douaniers plus efficaces

La douane a pour principale tâche d'exercer des contrôles efficaces en vue de prévenir le non paiement des droits et taxes, de réprimer la fraude et la contrebande, d'appliquer la politique commerciale et de faire respecter une série de prescriptions concernant la protection publique.

Pour pouvoir s'acquitter de ces responsabilités, la douane est tenue d'intervenir, régulièrement, dans le mouvement des marchandises aux frontières nationales afin de les examiner et/ou d'examiner les informations y relatives.

Compte tenu des ressources limitées dont dispose la douane et des exigences des délais actuels du commerce, il est normalement impossible de créer une situation où le risque serait nul en interceptant et en examinant tous les envois qui pénètrent ou qui quittent le territoire. La douane des principales nations commerçantes est donc devenue experte dans l'utilisation des techniques modernes de gestion des risques, élaborées et appliquées avec soin pour sélectionner et cibler les personnes et les envois suspects.

Les sous-programmes d'évaluation des risques et de sélection, destinés à identifier les envois devant faire l'objet d'une vérification documentaire et matérielle peuvent être appliqués dans le cadre d'un système manuel, mais ils sont réalisés de manière beaucoup plus cohérente, fiable et mieux documentée par les administrations qui ont informatisé leurs systèmes de contrôle des voyageurs, des transporteurs, des moyens de transport et du fret et/ou de traitement des déclarations de marchandises.

Des renseignements récents, recueillis par la douane, peuvent être introduits dans le système informatique pour compléter les données historiques, notamment les antécédents des entreprises en matière de respect de la loi, et orienter la sélection et le ciblage. Cette analyse systématique et précise des dossiers en temps opportun peut augmenter considérablement les chances de la douane de détecter et de réprimer des pratiques frauduleuses. L'un des avantages connexes de l'informatisation est qu'elle contribue également à déceler les transactions à l'importation dans le cadre desquelles la valeur déclarée des produits ne s'inscrit pas dans les paramètres prédéterminés.

2.3 Dédouanement plus efficace

L'informatisation du contrôle des voyageurs et des marchandises permet :

- d'améliorer la productivité de la douane et des entreprises;
- de rationaliser l'utilisation des ressources officielles et celles des entreprises;
- d'inciter les entreprises concurrentes à améliorer leurs propres dispositifs de protection nécessaires pour offrir aux entreprises qui respectent la loi des procédures préférentielles qui amélioreront leurs opérations commerciales et leur degré de respect de la loi;
- de réduire les coûts supportés tant par la douane que par les opérateurs commerciaux en accélérant l'octroi de la mainlevée des marchandises;
- de réunir à temps des informations plus précises;
- de disposer de capacités plus fiables en matière de lutte contre la fraude;
- de réduire la congestion des ports et des aéroports.

L'informatisation des procédures douanières et l'échange électronique d'informations, par exemple les données sur le fret et les déclarations de marchandises, ouvrent la voie au traitement des informations avant l'arrivée et/ou avant le départ. La saisie et la vérification des données officielles avant l'arrivée des envois à l'exportation ou à l'importation, au point de contrôle matériel de la douane, permettent aux administrations de procéder à une

première évaluation des risques et de notifier par voie électronique les décisions concernant le statut de la mainlevée des marchandises dès leur arrivée.

L'utilisation appropriée de la technologie de l'information et de la communication dans le cadre des accords de coopération conclus entre la douane, les autres services officiels et les déclarants peut permettre à toutes les parties à une transaction à l'importation/exportation d'utiliser un procédé à guichet électronique unique grâce auquel les services officiels de contrôle des frontières peuvent partager les données de contrôle exigées pour offrir aux entreprises une procédure de mainlevée/dédouanement rationalisée, toutes les formalités étant regroupées en un seul point.

2.4 Application uniforme de la législation douanière

Les règlements régissant les responsabilités et les prérogatives de la douane sont toujours plus nombreux et plus complexes. Dans un environnement manuel, la douane peut éprouver des difficultés à s'assurer qu'elle a tenu compte de tous les règlements en vigueur lors du traitement individuel de chaque envoi à l'importation ou à l'exportation. En revanche, un système informatique bien conçu, entièrement programmé pour ce qui est de toutes les prescriptions officielles à remplir, peut permettre de traiter toutes les transactions en accord complet et cohérent avec toutes les exigences légales. Tous les opérateurs commerciaux sont ainsi assurés d'une application uniforme de la législation nationale. La douane peut également utiliser les normes de données internationales et les techniques de modélisation pour offrir un traitement aussi uniforme et équitable dans le cadre des règles commerciales, de manière à ce que, lorsque la législation change, les règles elles-mêmes changent également.

2.5 Recouvrement plus efficace des recettes

Pour de nombreux pays, les droits et taxes à l'importation constituent la principale source de recettes publiques. Le recouvrement et la comptabilisation efficaces et en temps voulu de ces recettes sont donc vitaux pour l'économie d'un pays. L'informatisation de la douane peut contribuer à répondre à ces besoins. Dans un environnement manuel, le rapprochement des créances à recouvrer est parfois lent et propice aux erreurs. L'informatisation peut aider à identifier et à quantifier, instantanément et à tout moment, les créances irrécouvrables ou à recouvrer, afin de prendre rapidement les mesures qui s'imposent.

2.6 Analyse plus efficace des données

La douane constitue la principale source des données concernant le commerce international exigées par les gouvernements aux fins des analyses économiques et des négociations en matière de politique commerciale, sur lesquelles les entreprises se fondent pour faciliter les études de marché et orienter les stratégies de vente.

L'évaluation et l'organisation appropriées de ces renseignements détaillés, réunis et conservés dans des systèmes manuels sur papier, sont laborieuses et longues. Le fait d'en extraire des données utiles, ayant un rapport entre elles, demande beaucoup de travail.

L'informatisation permet d'obtenir des données commerciales à jour en tant que sous-produit virtuel du traitement des exportations et des importations. La douane peut offrir les avantages qui en résultent à tous les utilisateurs en aval et appliquer les outils de renseignement opérationnel pour interpréter et exploiter ces données en vue d'améliorer ses propres opérations à l'échelon national et local, s'agissant notamment de l'efficacité des contrôles a posteriori.

Les entreprises qui utilisent la TI sont en mesure de communiquer à la douane, en temps opportun, des données exemptes d'erreur, et la douane peut pour sa part se fier à la précision de ces données à ce moment précis et à tout moment ultérieur de leur analyse, grâce aux contrôles de validation et de crédibilité qui font partie intégrante du processus de saisie informatique.

2.7 Efficacité de l'établissement des statistiques du commerce extérieur

Pratiquement toutes les administrations des douanes sont chargées de recueillir les données commerciales qui servent de base pour établir les statistiques nationales du commerce extérieur et documenter toute une série de décisions importantes sur le plan politique et économique. Les données nécessaires sont généralement extraites des déclarations de marchandises à l'importation et à l'exportation. Dans un système informatisé, elles peuvent être présentées immédiatement selon la structure et la forme prescrites, et être d'un degré de précision très élevé, alors que, dans les systèmes manuels, elles ne deviennent disponibles qu'à un stade ultérieur du processus de dédouanement. Ces sous-programmes informatiques de la douane sont rentables et les statistiques établies grâce à eux permettent aux autres services publics de prendre rapidement des mesures.

2.8 Meilleure qualité des données

Les contrôles de validation et de crédibilité des données effectués au moment de la saisie permettent à la douane de supprimer les incohérences alors que les marchandises sont encore placées directement sous son contrôle et de s'assurer de la fiabilité des principales données de base introduites dans son système informatique à toutes fins ultérieures.

La validation des données, qui vise à protéger une application informatique contre l'introduction d'informations erronées, revêt la plus haute importance. Une fois que des données incorrectes sont saisies dans le système, les résultats de toute analyse deviennent sans valeur et les investissements financiers et en ressources autres ne produisent pas les résultats escomptés.

3. LE PROCESSUS DE DECISION

(Norme transitoire 7.1)

Pourquoi une administration des douanes ou toute autre organisation souhaite-t-elle introduire la TIC dans ses opérations? Accroître l'efficacité, résoudre un problème qui se pose, répondre à de nouveaux impératifs, pour la douane par exemple, mettre en oeuvre la Convention de Kyoto révisée, sont les raisons les plus fréquemment citées. Ce sont toutes des raisons parfaitement rationnelles.

Il en existe cependant de nombreuses autres, peut-être moins aisées à avouer et à formuler, mais qui sont tout aussi valables, par exemple le renforcement de l'éthique professionnelle.

Tous les projets d'informatisation doivent être abordés avec beaucoup de prudence, compte tenu des graves pertes financières et autres que peuvent entraîner des erreurs de planification et de gestion. Cette remarque ne vise absolument pas à dissuader les administrations d'utiliser des systèmes informatiques, mais seulement à les avertir des éventuels pièges et leur permettre, si elles prennent soin d'éviter ces pièges suffisamment tôt dans le processus de planification du projet, de progresser ensuite en toute confiance.

Le processus d'informatisation, depuis le moment où les cadres supérieurs se prononcent en sa faveur jusqu'au moment où un système informatique est mis en service et fonctionne réellement, appelle de longs travaux spécialisés de planification et de suivi, que le nouveau système soit mis au point par des fonctionnaires de l'administration ou par des consultants externes.

Compte tenu de l'ampleur des dépenses en matériel, en services et en effectifs qui sont invariablement liées à la conception et à la mise en place d'un système informatique douanier (y compris les interfaces et les systèmes de 'guichet unique' avec les autres services gouvernementaux), ainsi que des changements importants à apporter parallèlement aux méthodes de fonctionnement et aux procédures de base, chaque projet de cette nature présente de grands risques.

Il est donc essentiel que ces projets soient soigneusement préparés et suivis afin de définir et d'évaluer les risques et les incertitudes, de les réduire ou de les éliminer chaque fois que possible, et d'assurer une mise en place sans problèmes, dans les délais prévus et sans dépassement de crédits. Un bon suivi, qui constitue la base d'une planification saine et exhaustive, devrait permettre aux cadres supérieurs de repérer rapidement si l'on s'écarte du programme prévu et de prendre les mesures correctives qui s'imposent.

3.1 Gestion du changement

Dans le cadre des structures sociales modernes, toutes les institutions, qu'elles soient gouvernementales, à but lucratif, à but non lucratif, dans le domaine de la santé ou de l'éducation, doivent faire face aux pressions croissantes exercées en faveur du changement et sont censées :

- Faire plus avec moins
- Le faire plus rapidement
- Etre souples
- Tout en maintenant ou en améliorant la qualité des produits ou des services, ou les deux à la fois.

Dans dix ans, au moins 25 % de toutes les connaissances actuelles seront obsolètes. La durée utile des nouvelles technologies est de dix-huit mois et ce délai diminue rapidement. Il ne suffit plus de revoir, d'améliorer ou de remettre en question les anciennes méthodes. Les administrations des douanes notamment doivent changer afin de réagir de manière raisonnable à l'évolution massive des pratiques et des tendances du commerce international.

Elles doivent répondre aux quatre questions essentielles ci-après :

1) Quels sont les éléments les plus importants pour les usagers (importateurs, exportateur, transporteurs, agent douane) ?
2) L'administration doit-elle changer pour tenir compte de la réponse à cette question ?
3) De quelle manière le changement sera utile à l'administration ?
4) De quelle manière les changements apportés par la douane permettront-il de répondre aux besoins plus larges du gouvernement?

3.1.1 Les dix étapes de la mise en œuvre du changement

Première étape : Examiner plus particulièrement les opérations pratiques et non pas la fonction.

Il est très important que la douane définisse les fonctions dont elle doit s'acquitter mais, une fois cette tâche effectuée, elle doit étudier les moyens à mettre en œuvre pour réaliser ses fonctions, parce que c'est au stade des opérations que l'administration entre en contact avec les usagers.

Deuxième étape : Mise au point d'un profil de traitement

Dans une administration, la plupart des travaux à accomplir ne font pas l'objet de documents. Il s'ensuit qu'il est extrêmement difficile de déterminer avec précision les améliorations à apporter. En élaborant des documents à ce sujet, la douane doit viser à respecter la règle 80 – 20. L'application de cette dernière est très utile lorsque des mesures sont prises en vue d'apporter des améliorations, parce que :

- 20% des opérations absorbent 80% des ressources
- 20% des activités dans le cadre de telle ou telle opération permettent d'obtenir 80% des résultats
- 20% des problèmes posés par une opération donnée peuvent supposer des changements.

L'administration peut rapidement déterminer les quelques opérations essentielles qui exigent beaucoup de ressources en élaborant un profil de traitement assorti de schémas d'activités et de tableaux des différentes activités à entreprendre.

Troisième étape : Tableau descriptif des tâches

Les tâches à exécuter sont-elles nouvelles ou ont-elles évolué? Dans la plupart des administrations des douanes, les procédures opérationnelles ont été définies il y a longtemps, et le temps à manqué pour procéder à un examen critique et les modifier. Tout ce qui a fait l'objet de documents a changé depuis longtemps. Il s'ensuit que la plupart des fonctionnaires n'ont jamais vu une représentation visuelle de leurs travaux et ne savent pas ce qui se passe en amont et en aval. Ils ne savent pas où ils se trouvent sur l'organigramme. Un tableau descriptif des tâches donne un aperçu concret de la manière dont les travaux sont effectués. Il montre :

- comment évoluent les travaux d'amont en aval
- qui exécute les différents travaux
- la succession des différentes tâches et les reprises d'activités
- les décisions prises et les pièces à l'appui

Quatrième étape : Evaluer les méthodes de travail

L'évaluation des méthodes de travail permet à la douane de connaître les résultats obtenus et de définir des objectifs à atteindre en ce qui concerne une amélioration de ces résultats. Les sept critères ci-après permettent de déterminer l'efficacité des méthodes de travail :

- coût de la méthode employée : coût total de chaque tâche exécutée
- coût unitaire des tâches exécutées – coût global de chaque tâché achevée
- pourcentage de tâches effectuées sans avoir dû être revues, remaniées ou écartées
- coût de la reprise des travaux : coût imputable aux travaux nécessaires pour régler les difficultés relevées
- délai de traitement : temps nécessaire pour exécuter une tâche (minutes, jours, semaines, mois)
- délai réel de traitement : temps consacré à la réalisation d'une tâche sans attente ni reprise des travaux
- nombre de personnes chargées de la réalisation d'une tâche.

Cinquième étape : Etude des autres méthodes de travail de la douane

Les propositions ou les méthodes de travail dans les autres administrations des douanes peuvent fournir des indications précieuses et permettre de gagner du temps, ainsi que d'éviter des erreurs.

Sixième étape : Remaniement des méthodes de travail

Compte tenu des renseignements obtenus en appliquant les cinq autres critères, la douane peut concevoir les nouvelles méthodes de travail en éliminant les doubles emplois et les chevauchements d'activités.

Septième étape : Equilibre entre les méthodes de travail et la technologie

Dans la plupart des administrations, les systèmes informatiques sont étroitement liés à la manière dont les travaux sont effectués. Toutefois, les techniques doivent être considérées comme un outil et non pas, en soi, comme le moteur du changement. En effet, l'informatisation d'une tâche ne rendra pas nécessairement une administration plus productive. Lorsqu'une administration informatise une méthode de travail inefficace, elle obtient simplement des résultats médiocres plus rapidement. Tout en améliorant les opérations et en exploitant la technologie, la douane doit veiller à examiner d'abord les méthodes de travail, afin que les recommandations de nature technique reposent sur les conclusions auxquelles elle sera parvenue.

Huitième étape : Gérer la modification des méthodes de travail

La douane doit gérer activement le changement et mettant en évidence et en évaluant les risques avant que toute modification ne soit apportée. Le changement peut avoir plusieurs conséquences. Ainsi, la douane doit examiner plus particulièrement les conséquences qui sont :

- hautement souhaitables, mais qui ne se présenteront probablement pas si certaines mesures ne sont pas prises,
- guère souhaitables, mais qui se présenteront probablement si l'on ne prête pas suffisamment attention.

Neuvième étape : Préparer les fonctionnaires et les usagers au changement

Aucune administration n'est à ce point mauvaise que personne ne l'aime telle qu'elle est. La plupart des personnes résistent au changement par crainte de ce que l'avenir leur réserve, et non pas parce qu'elles sont réellement attachées au passé ou aux méthodes de travail actuelles. Le rôle de ceux qui dirigent le changement est difficile et ingrat. Il y a peu de cours de formation disponibles et peu de modèles dont on puisse s'inspirer. Les fonctionnaires peuvent devoir être guidés dans un processus en trois phases avant d'accepter sans réserve un changement prévu :

1. TETE :
   Les intéressés comprennent intellectuellement qu'il faut opérer un changement, compte tenu des éléments présentés à l'appui. Une participation aussi large que possible les aidera à mieux comprendre.
2. COEUR :
   Les intéressés participent sur le plan émotionnel au changement, en raison des résultats possibles.
3. PIEDS :
   Les intéressés s'engagent en tant que participants et non pas en tant qu'observateurs.

La durée du passage par chaque étape diffère selon les personnes et la situation.

Dixième étape : Poursuivre l'amélioration des méthodes de travail

Toute modification des méthodes de travail est longue, coûteuse et ardue. Bien que le changement s'impose parfois, si l'on apporte en permanence des modifications aux méthodes de travail, de petites améliorations interviennent tout le temps, les changements profonds étant apportés moins fréquemment. Les tâches ci-après doivent être exécutées par tous les fonctionnaires des douanes :

- évaluation permanente de la situation, en évaluant les méthodes de travail compte tenu de l'avis des usagers.
- rechercher les améliorations possibles, en se concentrant sur les améliorations qui permettent d'obtenir les meilleurs résultats.
- veiller à ce que des mesures soient prises lorsque les possibilités d'améliorations ont été mises en évidence et montrer que des résultats concrets ont été obtenus rapidement.
- évaluer les résultats, en transformant les modifications apportées aux méthodes de travail en résultats quantifiables.

Il n'y a pas de formule magique ou de formule miracle pour créer et maintenir une bonne gestion du changement. La douane doit être en permanence attentive aux améliorations compte tenu des problèmes et des possibilités qui se présentent tous les jours.

3.1.2 Raisons pour lesquelles le changement échoue

Information et communication inadéquates – la mauvaise qualité de la communication et du partage d'informations avec la partie prenante est souvent à l'origine de l'échec de la gestion du changement.

Le changement est trop long et trop coûteux. Lorsque le changement s'étale sur une longue période, on en oublie les objectifs, le financement et l'élan est perdu.

Il y a toujours des risques : tous les changements importants présentent des risques. Si les risques ne sont pas clairement mis en évidence, ils créeront un sentiment d'incertitude, d'ambiguïté et la crainte de l'échec.

La méthode à suivre n'est pas garantie : tout changement est difficile et complexe, il ne sera pas couronné de succès, si la méthode suivie est inconnue des fonctionnaires et qu'ils en prennent connaissance au fur et à mesure qu'ils progressent.

Les moyens disponibles sont insuffisants : tout changement réussi implique un programme de gestion des moyens pour s'assurer que leur ampleur a été définie, ainsi qu'un programme de recrutement qui permet de veiller à ce que le meilleur personnel disponible puisse être mis en place. Toutefois, il arrive que ces moyens soient les plus difficiles à obtenir.

Le regard est tourné exclusivement vers l'intérieur : de nombreux changements viennent de l'intérieur et non pas de l'extérieur. Or, si l'on ne tient pas compte de l'avis des usagers, il y a fort peu de chances que le changement soit couronné de succès.

Le changement provoque des perturbations : par le passé certaines administrations pouvaient suspendre le déroulement de certaines opérations pendant qu'elles opéraient des changements. Aujourd'hui, compte tenu du rythme soutenu auquel la douane doit faire face, nous sommes tous censés exercer notre activité en continu, car il est impossible d'arrêter le

travail pendant que des remaniements sont apportés aux méthodes de travail. Il s'ensuit qu'il importe de prévoir suffisamment de personnel de façon que rien ne soit modifié pendant que les nouvelles opérations se poursuivent également. On peut affirmer que les résultats ne sont pas bons lorsque le changement perturbe l'activité normale et que la productivité en souffre, ou si les fonctionnaires ne participent pas aux changements, c'est-à-dire qu'ils ne peuvent pas exécuter les anciennes tâches ou les nouvelles tâches.

3.1.3 Comment garantir le succès

Accélérer le rythme : les personnes qui conduisent le changement, de même que celles pour lesquelles il a une incidence, doivent voir des résultats concrets rapidement.

Appliquer une méthode qui a fait ses preuves : une méthode qui a fait ses preuves et qui a été appliquée par du personnel expérimenté dans ce domaine permet de ne pas avancer à tâtons. Les avantages qui doivent être obtenus sont clairement définis et communiqués aux intéressés. Ces derniers travaillent avec plus d'acharnement pour supprimer les barrières auxquelles se heurte le changement lorsqu'ils constatent que les efforts qu'ils déploient permettent d'obtenir des résultats concrets.

Tenir compte des usagers : les usagers seront les critiques les plus acerbes de votre administration. Par conséquent s'ils estiment que les modifications que vous apportez revêtent un intérêt, le changement est réussi.

Veiller à réduire au minimum les perturbations : le changement qui n'est pas géré et pour lequel des moyens n'ont pas été prévus peut provoquer des perturbations telles qu'il peut paralyser toute activité.

En résumé, pour garantir le succès d'un changement, les impératifs ci-après doivent être respectés :

- définir les besoins de l'administration en matière de changement
- mettre en place un dispositif structuré
- créer une équipe très qualifiée pour le gérer et mettre en œuvre le changement
- retenir les méthodes de travail appropriées qui doivent faire l'objet d'un changement
- être conscients des risques et mettre en place un programme de remplacement.
- informer le personnel et les usagers qu'un changement est en cours et les amener à y participer.

3.2 A qui confier la conception du système ?

L'informatisation d'une administration des douanes est une opération complexe et hautement spécialisée. Si le service ne dispose pas d'un personnel suffisamment formé et qualifié, il faut réfléchir avec soin à la question de savoir à qui cette tâche sera confiée.

Trois possibilités existent généralement : recruter un personnel suffisamment qualifié, former des fonctionnaires des douanes appartenant déjà à l'administration ou faire appel aux services d'une entreprise de consultants externes. Chacune de ces options présente des avantages et inconvénients.

Le recrutement d'un personnel qualifié soulève de nombreux problèmes, encore qu'il ait pour avantage que les travaux peuvent être engagés relativement rapidement. Les barèmes de traitements devront être suffisamment attrayants pour attirer un personnel suffisamment qualifié. Cet impératif constitue évidemment une source de conflits entre le nouveau personnel informatique et le personnel déjà en place, ce qui risque de compromettre le succès du projet.

La formation des fonctionnaires des douanes appartenant déjà à l'administration pour en faire des analystes de système, des programmeurs et des opérateurs offre peut-être une meilleure solution car ce personnel pourra tirer parti de son expérience douanière pour résoudre les problèmes qui se poseront. Il risque parfois de s'avérer difficile de conserver ce personnel lorsqu'il a acquis les qualifications professionnelles d'un informaticien, après l'investissement coûteux que représente la formation d'un personnel spécialisé. Une politique salariale appropriée doit donc être mise en oeuvre pour éviter que le personnel formé sur place ne se mette au service de sociétés privées.

La dernière option consiste à engager par contrat une société de consultants externes pour obtenir des conseils et une assistance aux fins de l'étude de faisabilité, de la sélection du matériel, de la conception des systèmes et de la programmation.

Les organisations qui s'informatisent pour la première fois choisissent souvent d'installer un système automatisé "clés en mains". Elles lancent donc des appels d'offres, compte tenu d'une étude de faisabilité, en vue d'obtenir un système opérationnel complet.

Les administrations disposant de leurs propres informaticiens lancent des appels d'offres pour se procurer le matériel, le logiciel et les moyens de communication, mais préfèrent parfois mettre au point leur propre logiciel d'application.

Dans ce cas, les appels d'offres s'adressent :

- - Aux fabricants d'ordinateurs avec logiciel
- - Aux fabricants d'ordinateurs sans logiciel
- - Aux entreprises de logiciels
- - Aux entreprises de systèmes
- - Aux services bureau opérant en différé
- - Aux servies bureau fonctionnant en temps partagé
- - A une combinaison des précédents.

Indications à fournir dans les soumissions :

- - Estimation du coût de la conception détaillée du système
- - Estimation du coût du travail de programmation
- - Frais de formation (tant pour les usagers du système que pour les analystes et les programmeurs chargés de son entretien)
- - Frais de matériel
- - Frais de communication
- - Frais d'entretien
- - Calendrier de mise en œuvre
- - Renseignements sur les activités et l'expérience de la société.

Il appartiendra ensuite à la direction des douanes d'évaluer les différentes propositions et de sélectionner la société qui sera chargée de concevoir, de programmer, de mettre à l'essai, d'installer et de mettre en œuvre le nouveau système. Il est indispensable qu'un Comité directeur conserve à chaque étape le contrôle des opérations au cours de la mise au point. Une société bien établie de réputation internationale sera probablement la mieux qualifiée pour installer un système "clés en mains". Cette option "clés en mains" risque d'être coûteuse, mais il est probable que les résultats seront plus rapides qu'avec les deux premières options.

Il est généralement souhaitable de créer un service informatique au sein de l'administration, même lorsque le système est mis au point par des consultants externes sur une base "clés en mains". Ce service doit être composé de fonctionnaires des douanes qui assureront la liaison entre les consultants et les services extérieurs de leur propre administration. Lorsque le système est en place et que les consultants sont partis, le service informatique est responsable de l'entretien du système. Il importe donc que ses membres soient formés de manière appropriée à l'informatique par les consultants externes ou par quelqu'un d'autre.

3.2.1 Choix d'un consultant

Lorsque l'administration des douanes décide de faire appel aux services d'un consultant, elle doit sélectionner celui-ci avec soin. Si son choix est malheureux, l'administration risque d'être liée par un contrat de longue durée qui pourrait s'avérer très peu rentable. La plupart des entreprises internationales de consultants en gestion font maintenant office de consultants en informatique, et elles offrent probablement la solution la plus sûre. Ces consultants jouent pour l'essentiel un rôle consultatif. Ils aident à choisir tel ou tel système et prouvent également écrire eux-mêmes le logiciel. Ils participent à la conception des appels d'offres et à l'évaluation des soumissions. Ils aident au recrutement du personnel et peuvent maintenir leur collaboration avec l'administration jusqu'à la mise en œuvre définitive du système.

Les consultants venant de l'extérieur peuvent échapper aux considérations de politique interne qui entravent et retardent souvent l'activité des équipes constituées avec le personnel de l'administration. Les consultants extérieurs doivent en outre être informés de manière appropriée et en temps opportun pour pouvoir s'adapter à la complexité du domaine douanier.

Les bons consultants ne sont pas bon marché, mais ils peuvent s'avérer rentables pour les administrations dépourvues du savoir-faire indispensable. En outre, leur contrat doit garantir qu'à leur départ, le personnel du service informatique de l'administration sera suffisamment formé pour les remplacer.

3.3 Comité directeur

Un élément essentiel du processus de planification est le Comité directeur du projet qui aura pour tâche d'entreprendre, de guider et d'étudier tous les projets d'informatisation. Le Comité directeur est composé de représentants de l'encadrement appartenant aux divers services de l'administration susceptibles d'être touchées. Le responsable du traitement des données, s'il en existe un au sein de l'administration, doit faire partie du comité, de même qu'un cadre supérieur des services financiers et comptables. La présidence doit être confiée à un

représentant de la direction, de préférence au directeur général des douanes ou à son adjoint, car les décisions concernant l'informatisation doivent être soutenues au plus haut niveau pour que leur exécution soit satisfaisante.

Dans de nombreuses administrations, les représentants de la direction au sein du Comité directeur n'auront pas les connaissances techniques voulues pour apprécier les problèmes que soulève le traitement des données et les impératifs qui en découlent. Il peut donc s'avérer souhaitable que les cadres supérieurs suivent des séances d'initiation à l'informatique spécialement conçues à l'intention des cadres et du personnel utilisateurs pour qu'ils puissent apprécier la nature des problèmes qui se posent dans un milieu informatisé. Il peut également s'avérer nécessaire d'engager un consultant indépendant qui fera partie du Comité directeur afin de conseiller la direction au cours des diverses phases de la mise au point du système.

3.4 Différents types de planification

Dans la plupart des organisations, et la douane ne fait pas exception, la planification informatique peut se répartir en trois catégories :

1. La planification stratégique (paragraphe 3.4.1.)

2. La planification des projets (paragraphe 3.4.2.)

3. La planification de la continuité des activités (paragraphe 3.4.3.)

3.4.1 Planification stratégique

Toutes les administrations des douanes appliquent un jeu commun de règles qui reflètent les procédures qu'elles utilisent aux fins de leurs opérations. Ces règles déterminent la manière de réaliser chaque procédure et influencent l'organisation administrative de la douane.

L'organisation administrative doit permettre que l'application de toutes les règles fasse l'objet des contrôles appropriés, à savoir, contrôle des activités, contrôles de nature financière, contrôle du personnel, organisation de l'ICP, etc.

La planification stratégique implique la mise au point du plan d'informatisation à long terme de l'administration. Les applications individuelles peuvent évidemment être automatisées en l'absence de tout plan à long terme, mais rien ne garantit qu'elles apporteront la solution la plus efficace aux problèmes de l'administration ou qu'elles seront compatibles avec les autres systèmes qui pourraient être conçus ultérieurement au sein de l'administration. Lorsqu'une administration s'est engagée dans une voie déterminée et installée dans une dépendance croissante par rapport à son système informatique, tout changement d'orientation peut s'avérer difficile et coûteux. Dans la plupart des administrations, l'adoption de l'ordinateur aura des répercussions sur plusieurs segments de l'organigramme et il est donc indispensable d'arrêter une politique intégrée pour que l'automatisation de l'administration se fasse de manière logique et cohérente, en évitant les doubles emplois et en réduisant les coûts au minimum.

Le plan stratégique ou à long terme de l'administration, qui fait généralement partie de l'étude de faisabilité ou qui fait immédiatement suite à ses conclusions, sera soumis au Comité directeur pour observations et approbation. Lorsqu'il aura approuvé le plan, le Comité directeur sera chargé d'en surveiller et d'en guider la mise en œuvre. Il attribuera un degré de priorité

aux divers projets définis dans le plan et appréciera les demandes formulées par les usagers en vue de nouveaux projets.

Le plan définit l'objectif auquel répondent les grandes orientations adoptées par l'administration en matière informatique, ainsi que les diverses applications à informatiser afin de réaliser cet objectif, leurs limites respectives et les interfaces à installer entre elles. Les aspects techniques du matériel, les langages de programmation, etc., seront également spécifiés.

3.4.2 Planification des projets

Le plan stratégique ou à long terme comprend plusieurs projets dont chacun appelle une planification et un contrôle individuels. Les projets sont généralement assignés à des équipes individuelles dont l'animateur rend régulièrement compte au Comité directeur. Dans certains cas, les comités de projet sont constitués sous la présidence de l'animateur qui fait à son tour rapport au Comité directeur. Lorsqu'une équipe a achevé un projet inscrit dans le plan à long terme, le Comité directeur lui en attribue un nouveau.

La planification individuelle de chaque projet est indispensable :

- pour en définir avec précision les objectifs et le cas échéant, les contraintes
- pour tracer les limites du projet
- pour en définir les relations avec les autres projets ou systèmes, déjà existants ou seulement proposés
- pour arrêter un calendrier précisant les tâches à accomplir, les personnes qui en seront chargées, la date de mise à exécution et les frais qui en résulteront.

La manière la plus facile de planifier et de contrôler un projet d'informatisation consiste probablement à le répartir en plusieurs phases faciles à gérer. La plupart des projets d'informatisation comprennent essentiellement trois phases :

1. une phase de lancement du projet
2. une phase de mise au point du projet
3. une phase faisant suite à la mise au point.

La phase de lancement comprend généralement l'étude initiale et l'étude de faisabilité dont il a été question au chapitre 5. Elle prend fin lorsque le Comité directeur se prononce en faveur de la mise à exécution du projet.

La phase de mise au point comprend les étapes suivantes :

- enquête détaillée et analyse du système actuel (paragraphe 5.1)
- conception détaillée du système (paragraphe 5.2)
- programmation (paragraphe 5.3)
- acquisition et installation du matériel (paragraphe 5.4)
- mise en oeuvre du système (paragraphe 5.5)
- évaluation (paragraphe 5.6)

Un grand nombre des étapes mentionnées ci-dessus sont entreprises consécutivement, et d'autres en parallèle; par exemple, l'acquisition et la mise à l'essai du matériel ont lieu

pendant les phases de conception détaillée et de programmation. En fait, l'acquisition et l'installation du matériel sont souvent considérées comme un projet en soi.

La phase consécutive à la mise en œuvre comprend l'entretien permanent du système et l'évaluation consécutive à la mise en œuvre.

La planification effective du projet d'informatisation appelle une estimation des ressources à consacrer à chaque étape et doit comprendre des délais convenus au préalable et l'attribution des ressources. La progression du projet est examinée au vu du plan de projet en divers points clés pendant toute la mise au point, tout écart par rapport au plan étant identifié et des mesures prises pour le rectifier. L'animateur du projet (ou le comité de projet) mesure constamment le rythme de progression par rapport au plan et fait rapport au Comité directeur à des intervalles convenus à l'avance. Dans certains cas, le Comité directeur ne peut consacrer de nouvelles ressources au projet que si les phases précédentes ont été réalisées convenablement et dans les délais.

La planification d'un projet d'informatisation n'est pas une tâche facile. Elle est encore plus difficile dans une organisation qui s'informatise pour la première fois. Toute administration qui entreprend un projet d'informatisation sans un plan d'action clair, tant à long terme qu'au niveau de chaque projet, sera rapidement amenée à constater qu'elle s'est égarée en chemin après avoir gaspillé des sommes importantes prélevées sur les fonds publics. Certes, la planification et le contrôle des projets ne garantissent pas le succès, mais ils permettent toutefois à la direction de maintenir un contrôle strict sur les ressources allouées et de minimiser les risques de dépenses ou de délais excessifs par rapport aux prévisions.

3.4.3 Planification de la continuité des activités

Il est conseillé aux administrations des douanes d'envisager l'utilisation de cadres normalisés pour gérer les projets, et notamment les projets de TIC à grande échelle. Outre les démarches traditionnelles de gestion des projets, plusieurs méthodologies et cadres ont été conçus, appuyés par des experts accrédités. PRINCE2 est un exemple de démarche structurée de gestion des projets. Des cadres comme HERMES peuvent être utilisés pour gérer les projets logiciels.

La planification de la continuité des activités est le processus global qui consiste à élaborer un plan d'action visant à ce que les activités en cours ne s'interrompent pas en cas de défaillance imprévue d'une fonction ou d'un système vital. Pour une administration des douanes, ce processus consiste à pouvoir poursuivre le recouvrement des droits et taxes, le contrôle des marchandises et des personnes franchissant les frontières et le dédouanement ininterrompu et rapide des biens et des personnes en trafic international.

Les administrations des douanes doivent en permanence se préoccuper de la continuité des activités. Si les systèmes ou les processus informatisés douaniers sont incapables de fonctionner :

- les marchandises non dédouanées risquent de paralyser des parties vitales de l'infrastructure d'un pays
- l'impossibilité de procéder à l'évaluation des risques peut soulever des risques particuliers pour la société
- les tentatives d'importation de marchandises faisant l'objet de restrictions risquent d'augmenter

- le public et les entreprises ne seront peut-être pas en mesure d'obtenir les renseignements dont ils besoin
- les calculs tarifaires risquent d'être erronés
- des erreurs peuvent survenir dans la perception et la comptabilisation des recettes et des droits.

C'est pour toutes ces raisons, et d'autres encore, que les administrations des douanes doivent disposer de plans de continuité solides. Faute de quoi, les ruptures pour les milieux industriels et la communauté en général pourraient nuire notamment à l'économie d'un pays ou d'une région, restreindre la capacité d'appliquer les lois et règlements, et l'approvisionnement du public en marchandises essentielles.

La planification de la continuité des activités doit faire partie intégrante de la gestion de toute administration des douanes, mais toutes les administrations n'ont pas mis en place un plan de cette nature.

Un plan de continuité des activités se composera d'une série de plans d'urgence adaptés à chaque activité et à chaque aspect de l'infrastructure. Chaque plan devrait être assorti d'une indication des ressources nécessaires, du rôle de toutes les catégories de personnel, des délais et des procédures à mettre en œuvre aux fins de sa réalisation. Ce processus se divise en quatre étapes :

1. Lancement
2. Analyse des risques et incidence sur les activités
3. Elaboration de plans individuels
4. Gestion des plans

Première étape : Lancement

- Obtenir l'engagement des hauts responsables
- Définir la politique et la portée de la gestion et de la continuité des activités
- Créer un Groupe de travail chargé du projet de "plan de continuité des activités"
- Elaborer un programme de référence avec des échéances

Deuxième étape : Incidence sur les activités et analyse des risques

- Définir des scénarios de pannes possibles dues à l'an 2000
- Définir les niveaux de résultat minimum acceptables pour chaque activité clé
- Evaluer l'incidence et les risques potentiels de ces scénarios sur les activités
- Définir et évaluer les différentes options

Troisième étape : Elaborer des plans individuels

- Définir et documenter des plans d'urgence et des modes de mise en œuvre
- Définir des éléments activant le déclenchement de chaque plan
- Allouer des ressources à chaque activité clé
- Obtenir l'approbation des responsables pour l'allocation des ressources

Quatrième étape : Gestion des plans

- Distribuer les plans à toutes les parties intéressées
- Assurer la tenue à jour de la stratégie, des plans et procédures
- Penser à la formation et à la sensibilisation nécessaires, examiner les plans et les risques, tester les plans, contrôler les changements apportés à la stratégie et aux plans afin d'assurer leur cohérence
- Former le personnel aux fins de la production d'une stratégie et de plans ainsi que l'exécution des mesures prévues par les plans
- Concevoir des plans de qualité qui soient applicables, c'est-à-dire qu'ils doivent être adaptables, complets, contenir des données concernant leur niveau qualitatif, leurs possibilités d'actualisation, leur niveau d'efficacité et de facilité de mise en œuvre (très important car le plan ne sera utilisé que dans une période de chaos ou de panne), leur fiabilité, leur résistance, le niveau de sécurité qu'ils permettent d'escompter, leurs possibilités de mise à l'essai et d'application en temps opportun, et les chances qu'ils ont d'être approuvés par les responsables.

Les administrations des douanes doivent obtenir, de la part des Ministres et des Directeurs de service, un engagement reconnaissant les éléments essentiels de la planification de la continuité des activités.

Un gestionnaire de la planification d'urgence, globalement responsable du plan de continuité des activités, doit être désigné. Etant donné qu'il s'agit d'un plan relatif à la survie de toute l'administration, il doit s'agir d'une personne dont l'autorité est suffisante pour obtenir que les différentes mesures prévues soient exécutées, pour exiger les ressources nécessaires, les répartir et coordonner les différentes mesures. Les détails du plan doivent être fournis par les responsables de chaque domaine d'activité.

Il pourra être nécessaire de désigner des coordinateurs régionaux ou locaux afin de gérer les différentes mesures de sauvegarde à l'échelon local. Chaque plan prévoira des mesures pour lutter contre certains risques. Il est conseillé de désigner à cette fin des personnes possédant les compétences voulues.

Pour plus de précisions sur la manière dont il convient de procéder pour assurer la planification de la continuité des activités, se référer aux directives de l'OMD sur la planification de la continuité des activités.

3.5 Elaboration d'une architecture d'entreprise :

La décision d'informatisation nécessite une planification scrupuleuse de la part des différents niveaux de l'organisation. La Section 3.4 évoque les différents types de planification, et notamment la planification stratégique, la planification de projets et la planification de la continuité des activités. L'élaboration de l''architecture d'entreprise' fait partie de la planification stratégique visant à introduire la Technologie de l'information et de la communication. Afin de contribuer au processus de gestion stratégique de l''entreprise', il est nécessaire de produire et d'actualiser les plans d'organisation pertinents.

L'architecture d'entreprise vise à établir des liens directs entre les impératifs commerciaux de l'entreprise et le déploiement technologique. A travers la mise en place de ces liens, l'organisation essaie d'aligner ses objectifs commerciaux et les solutions des

technologies de l'information. Cela favorise une utilisation optimale des ressources et l'identification des ressources qui ne contribuent pas aux objectifs commerciaux de l'organisation. L'absence de solution architecturale peut conduire à la prolifération de projets qui ne résolvent en rien les problèmes de l'organisation, de solutions qui font double-emploi et d'infrastructures inutiles qui ne contribuent nullement à atteindre les objectifs de l'organisation. L'architecture d'entreprise permet une utilisation plus efficace de la TIC, garantissant un meilleur rendement des actifs et un coût total de possession moindre. Par nature, il est risqué d'investir dans la technologie de l'information sans disposer d'une architecture d'entreprise.

L'architecture d'entreprise comprend différentes perspectives et descriptions architecturales qui soutiennent la planification de haut niveau pour des solutions prévoyant le recours à la Technologie de l'information. Différents cadres normalisés offrent une description des points de vue architecturaux. Par exemple, le modèle d'architecture du département américain de la défense (appelé DODAF) utilise trois points de vue : il s'agit i) du *point de vue opérations* qui identifie les activités à réaliser et qui les réalise, ii) du *point de vue systèmes* qui définit les systèmes répondant aux besoins opérationnels tout en se focalisant sur les échanges d'informations, et iii) du *point de vue normes techniques* qui définit les normes, notations et conventions techniques applicables. Ces trois point de vue sont interdépendants et contribuent, ensemble, au tableau final.

Les descriptions de l'architecture d'entreprise comprennent l'*architecture opérationnelle* ou *d'entreprise* qui décrit les fonctions de l'organisation et la manière dont elle s'acquitte de ces tâches. Par exemple, où et comment un fonctionnaire de la douane assure-t-il ;la vérification des documents et l'examen des marchandises ? Qui se charge du contrôle depuis le bureau des déclarations en douane et quels outils utilise-t-il ? Comment ces activités profitent-elles à l'organisation ? L'architecture de l'information donne une image globale du flux de l'information tant à l'intérieur de l'entreprise qu'entre les différentes entreprises. Elle comprend aussi le modèle conceptuel sous-jacent de données. L'inventaire des applications logicielles qui permettent d'atteindre les objectifs et les missions opérationnels de l'organisation fait partie de l'*architecture d'application*. Cette approche de l'architecture décrit comment les applications s'accordent entre elles et s'inscrivent dans l'objectif opérationnel global de l'organisation. La plate-forme logicielle qui se charge de la médiation entre les applications est appelée middleware ou logiciels des couches intermédiaires et fournit l'environnement logiciel nécessaire à l'exécution des applications. *L'architecture technologique* gère ces problèmes et régit d'autres architectures comme celles liées à la sécurité et aux logiciels. Ces points de vue architecturaux peuvent aider à rapprocher divers groupes au sein d'une organisation et contribuer à créer un consensus sur des besoins communs. Ils aident les participants au projet à comprendre des éléments concrets quant à ce qui est convenu pour le futur et quant à la manière de procéder.

Le Cadre de Open Group Architecture (TOGAF ®) est un cadre d'architecture d'entreprise qui offre une approche globale pour la conception, la planification, la mise en œuvre, et de gouverner une architecture d'information d'entreprise. Le cadre de mise en œuvre du guichet unique, un document produit par la CESAP / ONU et la CEE a été développé basé sur le concept TOGAF Enterprise Architecture. TOGAF est une discipline bien connue soutenu par un corps large et diversifié de praticiens.

Les présentes Directives recommandent que, dans le cadre de la planification stratégique de l'informatisation, les administrations douanières investissent dans l'architecture d'entreprise et fassent connaître aux planificateurs du projet et des opérations les descriptions et les points de vue architecturaux pertinents. Des échanges approfondis sur le concept et l'application de l'architecture d'entreprise peuvent être consultés dans le Chapitre 8 du Recueil de l'OMD sur le renforcement des capacités [publié par l'OMD en 2009] ainsi que dans le Chapitre 6 du Volume 2 du Recueil de l'OMD intitulé "Comment construire un environnement de Guichet unique" [publié en 2011].

4. IMPORTANCE DES CONSULTATIONS

(Normes transitoires 6.10 et 7.1)

Les systèmes informatiques douaniers ne peuvent être mis au point avec succès sans la coopération et la bonne volonté d'un grand nombre de personnes. Deux catégories particulièrement importantes doivent être consultées avant, pendant et après la mise au point : les entreprises et les fonctionnaires des douanes qui utiliseront le nouveau système

4.1 Les entreprises

Dans la mesure où la plupart des systèmes informatiques douaniers auront également une incidence majeure sur les autres usagers, les consultations avec les entreprises présentent une importance primordiale pour obtenir le maximum d'avantages. Un comité consultatif peut être officiellement créé pour donner des avis sur les questions d'ordre pratique et tenir les autres intervenants informés des intentions de la douane. Les autres administrations intéressées, les importateurs, les exportateurs, les transporteurs, les transitaires, les agents en douane, les autorités portuaires et aéroportuaires, etc., doivent être représentés au sein de ce comité.

4.2 Les fonctionnaires des douanes

Tout nouveau système informatique risque toujours de provoquer la résistance des usagers due à une réaction naturelle qui tente de résister au changement et de préserver le statu quo. Le meilleur moyen de surmonter cette résistance et d'assurer le fonctionnement le plus efficace possible du système est la participation et la coopération des usagers à toutes les étapes de la mise en route du nouveau système. Si un nouveau système est utilisé à mauvais escient, c'est généralement parce que ses utilisateurs ne l'ont pas bien compris ou ne souhaitent pas qu'il fonctionne.

Si les usagers ont le sentiment que le système ne répond pas à leurs besoins, c'est généralement parce que les recherches ont été insuffisantes ou que ces besoins ont été mal perçus par l'analyste du système revêt donc une importance cruciale car elle favorise l'efficacité de l'analyse et de la conception, elle facilite la compréhension par l'usager et lui inspire confiance et elle peut mettre en évidence les points qui risquent de soulever des difficultés. Les arguments qui militent en faveur de la participation sont manifestes, mais il n'est pas aussi simple de la faire passer dans les faits.

Pour que les usagers apportent une coopération efficace, ils doivent tout d'abord être convaincus de la sécurité de leur emploi. Les préoccupations qu'ils pourraient éprouver à cet égard doivent être dissipées d'emblée. Ils doivent faire confiance à l'analyste de système et être convaincus de sa compétence. Réciproquement, l'analyste de système doit faire confiance aux usagers et accepter leurs suggestions.

Les usagers doivent être tenus informés de ce qui se passe durant toute la durée du projet. Le manque d'information suscite les rumeurs et le mécontentement, créant ainsi une atmosphère des plus favorables à l'adoption d'un nouveau système informatique.

Des contacts réguliers sont indispensables pour inspirer confiance à l'usager et l'amener à coopérer. Les usagers doivent être convenablement représentés au sein des équipes et des comités chargés des projets. Des réunions de travail doivent être encouragées pour participer à la conception du nouveau système. En raison de leur connaissance approfondie et de leur compréhension du système manuel, ils peuvent apporter une importante contribution dans plusieurs domaines, par exemple, la disposition des bureaux, la conception des formules, les procédures de rectification des erreurs, la présentation des images sur écran, la présentation des états, etc.

L'éducation est également un élément important propre à favoriser la coopération de l'usager et à lui inspirer confiance. L'éducation de l'usager porte sur deux points. Le premier a trait à la connaissance générale de l'informatique et des notions fondamentales de cette discipline. Le deuxième concerne la formation approfondie à l'utilisation du système en cours de mise au point. Lorsqu'une entreprise extérieure met au point le système, la formation des usagers doit également faire partie de ses responsabilités.

Le succès ou l'échec du système dépend dans une large mesure de la coopération des usagers. Les chances de succès seront améliorées s'ils sont tenus informés, si on les rassure et si on les fait participer à la conception du système. Si l'usager est mis à l'écart, le système est voué à l'échec.

5. PROCESSUS DE MISE AU POINT DES SYSTEMES

(Normes transitoires 1.3, 6.8 et 7.3)

Dès qu'une solution a été adoptée compte tenu de l'étude de faisabilité et que l'autorisation financière indispensable est obtenue, le projet passe alors à la phase de la mise au point ; le système proposé qui n'était qu'un schéma théorique se concrétise alors sous la forme d'un système prêt à entrer en exploitation. Les responsables de la phase de mise au point seront naturellement désignés compte tenu de la vision stratégique de l'administration des douanes concernant les achats en matière de TI et des dispositions en vigueur au sein de l'administration pour ce qui est du personnel informatique (voir 5.1).

Au cours de cette phase comme au cours de toutes les autres phases de la mise au point du système, la direction doit contrôler étroitement l'évolution des travaux par l'intermédiaire du Comité directeur afin de veiller à ce que le projet progresse conformément aux délais qui ont été convenus et sans dépassement budgétaire. Il importe en outre que le produit obtenu au terme de cette phase demeure parfaitement maîtrisé à savoir les programmes informatiques et la documentation qui les accompagne.

Les programmes reproduisent dans le plus grand détail les procédures manuelles, et il faut donc absolument veiller à la fidélité de la reproduction, sinon le système obtenu en fin de compte ne répondra pas aux besoins des usagers.

Pour faciliter le contrôle par les usagers et la direction, cette phase de mise au point doit être répartie en plusieurs sous phases, les résultats de chacune d'entre elles étant étudiés par le comité de projet et le comité directeur avant que l'autorisation ne soit donnée de passer à la prochaine. Les diverses étapes de ce processus sont décrites dans le présent chapitre.

5.1 Enquête détaillée et analyse du système existant

Cette enquête détaillée portant sur les procédures existantes ne signifie pas que celle qui a été effectuée dans le cadre de l'étude de faisabilité est inexacte mais elle doit être beaucoup plus approfondie et ses résultats fourniront la base de l'analyse et de la conception détaillées du nouveau système.

La méthodologie utilisée pour l'enquête détaillée conduit pour l'essentiel l'analyste de système à interroger le personnel à tous les niveaux de l'administration et à consulter également les manuels administratifs et tous les autres documents utiles qui pourraient être disponibles. Ayant réuni tous les faits, l'analyste de système analyse ensuite tous les renseignements qu'il a recueillis et arrête un cahier des charges qui sera soumis au comité de projet puis au Comité directeur. Ce document indique dans un langage accessible au profane les principales caractéristiques du nouveau système et les incidences qui en résulteront pour l'encadrement et le personnel.

A ce stade, le comité de projet devra faire participer pleinement les usagers à la mise au point du système afin de vérifier l'exactitude des renseignements recueillis par l'analyste de système et de s'assurer que la conception détaillée du nouveau système peut être entreprise

sans qu'il devienne nécessaire ultérieurement d'y apporter des modifications. En effet, les usagers devront dire à l'analyste si le système qu'il est en train de concevoir répond à leurs besoins.

Le cahier des charges devra être approuvé par le comité directeur avant que la conception détaillée ne soit entreprise et ne devra plus appeler aucune mise à jour lorsque le contenu en aura été arrêté d'un commun accord. Le cahier des charges fournit souvent aux usagers une dernière occasion de demander des changements lorsque la conception de système ne répond pas à leurs besoins. Une fois arrêté, il est souvent réputé "gelé", c'est-à-dire qu'aucune modification ne peut plus y être apportée par la suite.

5.2 Conception détaillée du système

La conception détaillée du système commence, après l'analyse, lorsque le comité directeur a autorisé la mise au point d'un nouveau système.

Cette autorisation s'appuie sur la conception simplifiée du système qui figure dans le rapport de faisabilité, accompagnée du relevé systématique des besoins des usagers qui figure dans le cahier des charges. Pour l'essentiel, la conception du système consiste à spécifier en détail les impératifs propres à l'ordinateur et au traitement manuel, les impératifs propres à l'ordinateur et au traitement manuel, les éléments à introduire dans le système, les éléments produits par lui, les fichiers informatiques servant à stoker l'information et la segmentation du traitement en programmes.

Le résultat de ce travail de conception se concrétise par une série de documents établis par l'analyste de système, à savoir:

- Spécifications de la suite des programmes
- Manuel de l'usager
- Manuel des opérations
- Données d'essai
- Instructions pour le changement de système.

Les spécifications de la suite de programmes fournissent au programmeur les renseignements voulus sur les fonctions informatiques du système pour écrire les programmes.

Le manuel de l'usager fournit aux services utilisateurs des instructions sur les opérations courantes qu'appelle le bon fonctionnement du système et les mesures à prendre en cas de panne ou d'erreur. Le manuel de l'usager doit pouvoir être consulté pendant toute la durée opérationnelle du système. Il doit refléter en permanence l'état de ce dernier et doit être mis à jour en cas de changements ayant une incidence sur les procédures à suivre par les usagers. Ceux d'entre eux qui n'ont pas une expérience préalable des systèmes informatiques ne réalisent généralement pas combien il importe de se conformer rigoureusement aux instructions figurant dans le manuel. Il faudra donc veiller attentivement à sensibiliser les usagers à ce sujet.

Le manuel des opérations est le document de référence permanent utilisé pour informer le service informatique sur le système à mettre en œuvre et les tâches qu'appellent les opérations de routine.

Lorsque les programmes sont écrits et que les usagers sont familiarisés avec les nouvelles procédures, le système devra être mis à l'essai pour en garantir le bon fonctionnement dans toutes les circonstances prévisibles de façon à obtenir les résultats voulus. Des données d'essai sont indispensables pour que le système une fois mis en place puisse être expérimenté à la satisfaction des concepteurs du système et de ses utilisateurs.

Enfin, deux jeux d'instructions sont indispensables pour le passage d'un système à l'autre, l'un à l'intention des services utilisateurs et l'autre à l'intention du service informatique. Ces instructions préciseront en détail les procédures nécessaires pour le passage de l'ancien au nouveau système.

Tous ces documents seront examinés par le comité de projet et le comité directeur avant que la mise en route de la programmation ne soit approuvée.

5.3 Programmation

La programmation comprend les opérations suivantes : conception de la structure et l'appui, codage, préparation d'un plan et de données d'essai, mise à l'essai (partie technique) et déblocage des programmes et établissement de la documentation définitive.

La programmation a pour point de départ les spécifications de la suite des programmes établies lors de la conception détaillée du système. Le programmeur met à l'essai ses propres programmes dans une certaine mesure; toutefois l'intégralité du système, y compris l'ensemble des programmes, devront être mis à l'essai pour être acceptés par l'usager et finalement approuvés par le comité de projet et le comité directeur avant la mise en exploitation du système. Du point de vue de la direction, il faut absolument veiller à ce que les programmes informatiques soient entièrement documentés. Les programmes non documentés ne doivent être acceptés sous aucun prétexte. Sans documentation à l'appui, les programmes sont pratiquement illisibles et ne peuvent être modifiés que par leur auteur.

On ne saurait trop souligner que la documentation est un élément fondamental de toute suite de programmes. Il est tout aussi fondamental que les programmeurs se conforment à des normes de programmation reconnues, sinon l'entretien risque de soulever des problèmes. Il faut souligner à l'intention des programmeurs que les programmes doivent fonctionner normalement et être faciles à modifier s'il y a lieu.

5.4 Le processus d'acquisition

5.4.1 Acquisition

Jusqu'à maintenant, la question du matériel informatique sur lequel le nouveau système sera exploité n'a pas été évoquée en détail. L'acquisition du matériel ne doit pas intervenir avant que l'étude de faisabilité et l'analyse détaillée ne soient achevées, ni après que le système a été conçu et programmé. Si l'acquisition d'un nouveau matériel s'impose, elle devra généralement intervenir parallèlement à la phase de conception du système.

Les administrations doivent éviter de tomber dans le piège qui consiste à acquérir un matériel coûteux avant d'avoir procédé à une étude détaillée de leurs besoins informatiques. Il est à craindre en effet que ce matériel ne réponde pas à leurs besoins et ne devienne simplement un coûteux boulet à traîner. Il n'est pas prudent non plus de reporter cette

acquisition après la programmation du système, ce qui ne ferait que prolonger la mise en œuvre du système automatisé. La plupart des organisations font en sorte que la livraison et l'installation du matériel coïncident avec la phase de programmation étant donné que c'est à ce moment que l'on a besoin de l'ordinateur.

Les administrations devront donc entreprendre l'acquisition du matériel suffisamment à temps pour qu'il soit disponible au moment voulu. L'acquisition d'un système informatique appelle l'achat de trois éléments essentiels (matériel, logiciel (systèmes et applications) et communications). Certaines administrations des douanes (notamment celles qui utilisent pour la première fois les TIC) opteront pour l'installation d'un système complet fourni « clés en mains ». Nous examinerons toutefois ici la procédure d'acquisition du matériel, du logiciel et du dispositif de communication indépendamment du logiciel d'application, et non pas l'acquisition d'un ensemble complet comme dans l'hypothèse « clés en mains ».

5.4.2 Appel d'offres

Pour se procurer le matériel nécessaire, les administrations adressent généralement un appel d'offres à une série de vendeurs réputés capables de présenter une proposition sérieuse. Toutefois, auparavant, il est indispensable d'établir un document qui précise les fonctions que le matériel doit être capable d'accomplir. Ce document est désigné sous le nom de spécifications fonctionnelles. Dans certains cas, le rapport d'étude de faisabilité peut suffire. Sinon, il faudra le compléter de façon à obtenir le minimum de renseignements ci-après

→Eléments obligatoires

- Liste de tous les éléments que le système informatique doit comporter, notamment pour être conforme aux normes informatiques;
- règles de compatibilité, si le système doit être utilisé conjointement avec un autre;
- capacité d'extension, si le volume de travail est susceptible d'augmenter au cours de la durée d'utilisation du système;
- possibilité de récupération en cas de panne;
- règles de sécurité, etc.
- toutes les conditions à remplir par le logiciel doivent être répertoriées.

→Répertoire détaillé des volumes de travail à prendre en charge

- Description des opérations à accomplir, des volumes de données à introduire, des volumes de traitement, des volumes de stockage; type de stockage (en ligne, en différé), durée du stockage, volume de pointe (pour les systèmes en ligne), temps de réponse (pour les systèmes en ligne), temps de retournement (pour les systèmes par lots).
- Interventions du vendeur
- Indication de toutes les interventions du vendeur : planification du site, installations électriques, conditionnement d'air, prévention de l'incendie, alimentation auxiliaire en électricité, calendriers d'installation, temps d'ordinateur fourni avant installation, essais de ligne, personnel de soutien sur place, formation et point particulièrement important, entretien.

→Fiabilité

- La fiabilité s'exprime généralement en pourcentage du temps d'exploitation prévu. Si l'on veut obtenir un indice de fiabilité très élevé, par exemple 99 %, le vendeur sera probablement contraint de proposer un système double. Il en résultera une augmentation considérable des frais, notamment si le contrat prévoit des pénalités substantielles en cas de panne d'une durée excessive. Par conséquent, il est préférable de déterminer la durée de panne tolérable pour demeurer à l'intérieur des critères auxquels doit répondre un système d'exploitation suffisamment souple. Il importe de prévoir au contrat des pénalités qui garantissent que le vendeur fournira l'entretien et le matériel voulus pour se conformer aux critères de fiabilité établis.

→Dispositions contractuelles

- Il s'agit des obligations contractuelles qui engagent tant l'administration que le vendeur. Elles précisent divers éléments comme les dates de livraison, les dates de paiement, les pénalités, le règlement des litiges, etc.

Outre les spécifications fonctionnelles qui reprennent tous les éléments ci-dessus, il est indispensable de soumettre un certain nombre de problèmes types d'évaluation aux fournisseurs éventuels pour que le matériel proposé réponde aux normes voulues. Un problème d'évaluation est une version simulée d'une application informatique type que le vendeur peut exploiter sur l'ordinateur à fournir. Les résultats feront partie de sa proposition définitive.

5.4.3 Evaluation des soumissions

Les propositions communiquées par les fournisseurs éventuels sont évaluées par le comité directeur (qui prendra s'il y a lieu l'avis d'un consultant spécialisé dans l'évaluation des soumissions) sous les rubriques suivantes :

- Evaluation technique
- Evaluation des coûts
- Evaluation des performances.

L'évaluation technique comporte un examen des soumissions destiné à en garantir la conformité avec l'appel d'offres.

L'évaluation des coûts consiste à établir une comparaison entre les offres des fournisseurs : coût en cas d'achat définitif, en cas de location-vente et en cas de location-vente avec option d'achat. Les diverses options offertes par chaque fournisseur doivent être examinées en détail de façon à déterminer la solution la plus rentable. Des essais et démonstrations en grandeur réelle doivent être organisés avec chaque fournisseur qui passe le cap de l'évaluation technique. Au cours des essais en grandeur réelle, les données de l'évaluation doivent être exploitées et les résultats réunis et appréciés.

Seuls les fournisseurs dont le matériel passe le cap des essais d'évaluation et répond aux impératifs techniques devront être pris en considération lorsqu'il s'agira d'attribuer le contrat. Des négociations doivent être entreprises avec chacun des fournisseurs afin d'obtenir le prix le plus avantageux.

Après une évaluation systématique de l'ensemble de soumissions, l'administration doit être en mesure de choisir un fournisseur et une configuration de matériel. Lorsque le moment

est venu de rédiger le contrat, l'administration doit insister pour que toutes les circonstances particulières et les offres d'assistance technique et de soutien ainsi que l'entretien du matériel soient expressément prévus. De même, si le fournisseur qui l'emporte a promis un soutien complémentaire au cours des phases suivant l'installation, la nature de ce soutien doit être soigneusement définie et prévue au contrat.

L'acquisition du matériel informatique se fait normalement par un contrat de location-vente auprès du constructeur, mais il existe également des plans d'achat et divers contrats de location-vente auprès de sociétés indépendantes spécialisées. Les répercussions financières de ces diverses options doivent être étudiées attentivement par les responsables des services financiers. En outre, le contrat doit être étudié par un juriste qui veillera à ce que les intérêts de l'administration soient suffisamment pris en compte.

5.4.4 Installation

L'installation de l'ordinateur peut être complexe et prendre beaucoup de temps. Il est facile de sous-estimer le temps et les ressources qu'elle exige pour être menée à bien. Les constructeurs sont fréquemment en mesure de fournir une liste répertoriant systématiquement les diverses activités à entreprendre avant la livraison du matériel. Sur cette base, il faut arrêter un plan qui indique les activités à entreprendre avant l'installation et leurs relations réciproques le cas échéant. Ces activités sont les suivantes:

- plan de préparation du site
- plan des effectifs
- plan de communication des données
- calendrier de livraison
- plan de soutien logistique

La préparation du site consiste à déterminer la superficie à attribuer au centre informatique et à la bandothèque, à définir les conditions de température et d'humidité, les branchements électriques et téléphoniques à prévoir, et à énumérer toutes les installations devant accompagner l'ordinateur comme les dispositifs anti-incendie, les protections contre les interférences électriques, les dispositifs de sécurité électroniques, les sources auxiliaires de courant électrique, etc. Il s'agit également de définir les différents équipements auxiliaires comme le mobilier, les rayonnages de bandes, les tapis, les plates-formes d'observation pour le contrôle, le matériel pour l'établissement des états, etc.

Le plan des effectifs indique tout le personnel requis pour faire fonctionner le centre informatique, la date à laquelle il devra être en fonction et les mesures de recrutement ou de mutation à prendre à cet effet. Un centre de traitement de l'information doit normalement être doté d'un directeur de centre des données, d'opérateurs sur ordinateur et de contrôleurs, de programmeurs sur logiciels, d'un personnel chargé de la préparation des données, d'un personnel chargé du contrôle technique (si l'application informatique appelle un dispositif élaboré de communication des données) et d'opérateurs chargés de la saisie *des données.*

Le plan des effectifs indique également la date du recrutement du personnel nouvellement engagé, la date de mise en route du recyclage pour le personnel existant qui devra être formé en conséquence, la date à partir de laquelle le personnel devra être disponible ainsi que la date à laquelle il prendra effectivement ses fonctions et la manière dont il devra s'en acquitter. Le plan des effectifs doit être coordonné avec le processus d'acquisition de façon que le personnel soit disponible au fur et à mesure des besoins.

Le plan de communication des données indique les besoins en matière de transmission des données et précise quand et comment les circuits de données, les modems et les concentrateurs seront installés à l'appui du système.

Un plan de soutien logistique est établi pour indiquer les soutiens nécessaires et la date à laquelle ils devront être fournis par l'extérieur, notamment pour le recrutement, les transports et déménagements, l'installation du matériel, l'assistance juridique, etc.

L'installation du système informatique relève normalement de la responsabilité du fournisseur des ordinateurs. En revanche, la préparation du site relève exclusivement de la responsabilité de l'administration des douanes et si le site n'est pas prêt à temps, le fournisseur n'est pas responsable des retards apportés à l'installation. De même, si le site n'est pas conforme aux prescriptions du fournisseur et que les écarts sont sensibles, le vendeur refusera généralement d'installer le système informatique tant que les rectifications voulues n'ont pas été apportées au site.

Une fois installé, l'ordinateur n'est pas considéré comme opérationnel tant qu'une série de tests n'a pas été entreprise pour vérifier qu'il demeure suffisamment performant pendant un délai prolongé. Ces essais revêtent une importance critique et exigent un personnel hautement qualifié. Si l'administration ne dispose pas du personnel voulu, il est préférable de confier cette tâche à un consultant indépendant. Lorsque l'ordinateur a passé les tests avec succès, il est déclaré "opérationnel".

5.5 Mise en oeuvre du système

La mise au point du système a maintenant atteint un point où l'ordinateur est installé et où les programmes sont écrits. La phase suivante est celle de la "mise en œuvre"; elle comprend en réalité un certain nombre d'activités ou de sous-phases, à savoir :

- Mise à l'essai du système
- Conversion des fichiers
- Formation de l'usager
- Transition.

5.5.1 Mise à l'essai du système

Lorsque les programmeurs se sont acquittés de leur tâche, les programmes et la documentation sont remis à l'équipe chargée du système pour essai. Il s'agit principalement de repérer et de rectifier les défauts qui peuvent encore entacher les programmes. Certains défauts peuvent être imputables à des malentendus entre l'analyste et l'usager ou bien entre l'analyste et le programmeur. Si de nombreux défauts sont imputables à des spécifications incorrectes, c'est que l'enquête, l'analyse et la conception n'ont pas été exécutées avec suffisamment de soin.

Le plan et le programme de travail des essais de système doivent être arrêtés par l'analyste et approuvés par le comité de projet. Lorsque le système est mis au point par des consultants externes, il est indispensable que le personnel de la douane apporte son entière participation pour s'assurer que le système répond à ses besoins. Les données d'essai, qui ont été préparées par l'analyste au cours de la phase de conception du système et qui simuleront

aussi fidèlement que possible les conditions réelles de fonctionnement, seront traitées par ordinateur. Les résultats seront ensuite comparés avec les prévisions et, le cas échéant, les causes des anomalies constatées seront recherchées jusqu'à ce que les résultats soient impeccables et exempts d'erreur. Même lorsque tous les essais ont été entrepris à la satisfaction de tous, il peut encore s'avérer nécessaire d'entreprendre de nouveaux essais en grandeur réelle - voir ci-après la "stratégie du changement".

5.5.2 Conversion des fichiers

Il s'agit de convertir les fichiers manuels en fichiers informatiques, soit en d'autres termes de convertir les données de référence et autres, par exemple le tarif douanier, sous une forme lisible par l'ordinateur; c'est là une tâche essentielle.

Les différentes catégories de fichiers informatiques pouvant être créés dans un système douanier sont par exemple les suivants:

- Fichier tarifaire
- Fichier des contingents
- Fichier des devises
- Fichier des pays
- Fichier des importateurs.

Lorsque ces fichiers sont constitués, ils appellent des mises à jour constantes jusqu'à ce que le système soit en exploitation, et devront continuer à être mis à jour pendant toute la durée de vie du système.

La conversion des fichiers appelle généralement la transcription des données initiales sous une forme qui se prête à l'introduction dans l'ordinateur. Lorsque les fichiers sont constitués, l'exactitude doit en être vérifiée car rien ne peut perturber le démarrage d'un nouveau système autant qu'un fichier principal défectueux. L'opération est coûteuse et prend beaucoup de temps. Elle doit être planifiée avec soin car elle conditionne le succès de l'ensemble du système.

5.5.3 Formation des usagers

Pour qu'un système fasse la preuve de son efficacité , toutes les personnes en cause qui seront chargées de faire fonctionner le système doivent être suffisamment formées. L'analogie avec le "maillon le plus faible de la chaîne" convient ici tout particulièrement.

La formation des usagers peut relever de la responsabilité de l'équipe chargée du système (lorsque le système est mis au point par l'administration elle-même), cette responsabilité peut être partagée avec le service du personnel de l'administration ou bien elle peut être confiée à des consultants externes lorsque ceux-ci sont chargés de la mise au point du système.

Cette formation se fait à deux niveaux :

1. Initiation à l'informatique en général

2. Apprentissage de l'utilisation du nouveau système.

Lorsque les usagers n'ont aucune expérience préalable de l'informatisation, leur initiation doit être entreprise aussitôt que possible (dès que le rapport de faisabilité est approuvé).

L'apprentissage de l'utilisation du nouveau système doit en revanche intervenir aussi tard que possible, de façon que les nouvelles formules et les nouvelles techniques ne soient pas oubliées au moment de la mise en oeuvre. Il est recommandé que la durée de la formation technique et de la mise en application des connaissances acquises ne dépasse pas deux semaines.

L'initiation aux conditions effectives d'utilisation du nouveau système doit porter sur les points suivants :

- Aperçu général de la logique du système.
- Saisie des données.
- Interprétation des données obtenues.
- Limites et contraintes du système.
- Mesures à prendre lorsque des erreurs sont signalées.
- Pratique de l'utilisation des données et des fichiers d'essai.

5.5.4 Stratégie du changement

Le système est maintenant conçu, programmé et testé, les fichiers sont convertis, les usagers sont formés. Il s'agit désormais d'exploiter le système en grandeur réelle.

Il existe trois stratégies fondamentales pour passer aux conditions d'exploitation réelles :

1. Exploitation en parallèle.
2. Exploitation pilote.
3. Transition directe.

L'exploitation en parallèle est souvent de la meilleure méthode pour un système informatique qui remplace dans toutes ses fonctions essentielles un système manuel reposant sur les documents papier. Le système manuel continue de fonctionner sans changement lorsque le système informatique est mis en service pour la première fois. Les résultats fournis par les deux systèmes sont comparés point par point jusqu'à ce que toutes les discordances soient résolues. Cette méthode n'est possible que si les deux systèmes ont une production identique pour l'essentiel et si les effectifs sont suffisants pour poursuivre l'exploitation de l'ancien système tout en préparant les données à introduire dans le nouveau et vérifier les résultats.

L'exploitation pilote est souvent préférable lorsque le nouveau système devra être installé dans plusieurs emplacements - ce qui est souvent le cas pour la douane. Un emplacement type est choisi pour l'essai pilote, là où le service chargé du traitement des données et en particulier l'équipe chargée du système peuvent concentrer leurs ressources jusqu'à ce que le système ait fait ses preuves dans les conditions réelles d'exploitation et que les principaux problèmes soient résolus. Le système peut alors être mis progressivement en service dans d'autres emplacements.

Si aucune des autres méthodes ne convient, la transition directe qui consiste à mettre fin à l'ancien système un jour bien déterminé et à mettre le nouveau en service dès le lendemain est la seule solution. Pour que l'opération réussisse, deux conditions doivent être remplies au préalable. La première est que le système informatique ait été testé intégralement avant d'être exploité avec des données réelles. La deuxième est l'existence de plans d'urgence en cas de

défaillance du nouveau système. Il faudra alors éventuellement conserver une copie des données introduites, établir la liste de tous les fichiers principaux à chaque mise à jour et maintenir en fonction le personnel dans le service utilisateur jusqu'à ce que le nouveau système ait fait ses preuves.

Chaque solution présente des avantages et des inconvénients. En cas de transition directe, l'usager et le système ne sont que modérément sollicités, mais les conséquences d'un échec peuvent être catastrophiques. En cas d'exploitation pilote ou en parallèle, le risque d'échec est beaucoup moins grand, encore que ces deux méthodes sollicitent plus fortement le système et l'usager. Dans le cas des grands systèmes, il peut s'avérer préférable de recourir à l'exploitation en parallèle dans un seul emplacement pilote. C'est là certainement l'option la plus sûre dans un domaine particulièrement sensible où un échec pourrait être extrêmement coûteux. L'exploitation pilote et l'exploitation en parallèle permettent de mettre à l'essai au moindre risque les parties du système qui n'ont pas encore été testées, à savoir les procédures de l'opérateur, les procédures de préparation des données, les procédures propres au service utilisateur, etc. Ces procédures auront été définies dans les manuels de l'opérateur et de l'usager par l'analyste au cours de la conception du système et devront être testées en grandeur réelle. Lorsque le nouveau système (tant les sous-systèmes informatiques que manuels) fonctionne de manière satisfaisante depuis un temps raisonnable, le comité directeur ordonne de mettre fin à l'ancien système manuel.

5.6 Evaluation postérieure à la mise en œuvre

(Norme transitoire 7.1)

L'évaluation postérieure à la mise en œuvre est une suite essentielle à tout projet d'informatisation. Les principales raisons qui la motivent sont les suivantes :

- déterminer dans quelle mesure le système informatique produit les effets voulus;
- veiller à la réalisation des avantages prévus, tangibles ou intangibles;
- comparer les coûts et avantages effectifs avec ceux qui étaient prévus au stade de l'étude de faisabilité;
- identifier les faiblesses du système et recommander les améliorations nécessaires.

L'évaluation postérieure à la mise en oeuvre est un élément essentiel du contrôle effectif du projet. Elle fournit à la direction des douanes une justification indépendante des frais de mise au point tout en attestant les avantages effectivement obtenus.

L'évaluation postérieure à la mise en oeuvre est généralement conduite pour le compte du comité directeur par le comité de projet encore que, dans certains cas, une équipe indépendante soit engagée à cet effet. De même, dans certains cas, l'évaluation peut être confiée à une autre administration comme le Ministère des finances ou le Trésor, qui peuvent exiger une justification officielle des dépenses engagées. En général, l'évaluation postérieure à la mise en oeuvre doit être entreprise environ 6 à 9 mois après l'entrée en service du système. Ce délai est suffisant pour régler les premières difficultés et pour que les usagers se familiarisent avec les nouvelles procédures. Il est également souhaitable que cette évaluation n'ait pas lieu qu'une seule fois mais se répète par intervalles de deux à trois ans de façon que le fonctionnement du système demeure constamment à l'étude.

Même si de légères modifications, améliorations ou adaptations sont parfois recommandées suite à une évaluation postérieure à la mise en oeuvre, il est rare qu'un projet soit abandonné ou foncièrement modifié sauf si les mécanismes de planification et de contrôle n'ont pas été mis en oeuvre convenablement.

La tâche de l'évaluateur peut être compliquée par certains problèmes qui risquent de se poser au cours de l'évaluation. En premier lieu, il arrive souvent que l'on ne dispose pas de données historiques suffisantes et convenablement documentées au sujet de l'ancien système manuel pour procéder à une comparaison valable avec le nouveau système. Le rapport d'étude de faisabilité fournit un certain nombre de renseignements sur le système manuel, mais ils sont souvent insuffisants. D'autres difficultés peuvent être dues aux espoirs excessifs mis par l'usager dans le nouveau système. Lorsqu'il n'est pas convenablement initié aux fondements de l'informatique, l'usager croit parfois que l'ordinateur peut résoudre tous ses problèmes par simple pression sur une manette. Or, c'est rarement le cas dans la réalité. Les changements apportés aux besoins de l'usager peuvent également provoquer des difficultés. Les usagers ne comprennent pas toujours que le système informatique ne peut être conçu qu'en fonction de la situation existant à l'époque. Si les impératifs changent, le système informatique doit également être modifié ou sa conception repensée.

L'appréciation quantitative de certains avantages du système soulève fréquemment un autre problème. Par exemple, il est difficile de quantifier les avantages de l'informatisation douanière pour l'économie d'un pays dans son ensemble. Il n'est pourtant pas excessif d'affirmer qu'elle présente certains avantages. Enfin, lorsque le système est évalué par un évaluateur indépendant qui n'appartient pas à l'administration des douanes, sa connaissance insuffisante du domaine fonctionnel à l'étude peut soulever des difficultés. Cette lacune peut parfois provoquer des malentendus et il faut veiller à ce que le rapport de l'évaluateur ne contienne aucune erreur de fait.

En dépit des difficultés, l'évaluation postérieure à la mise en oeuvre présente plusieurs avantages. En premier lieu, elle fournit aux usagers l'occasion de faire valoir leur point de vue sur le système et d'indiquer s'il répond ou non à leurs besoins. S'ils ont des critiques justifiées à formuler, le rapport de l'évaluateur fournit une base qui permettra de rectifier le cas échéant les lacunes du système. Il fournira également une occasion d'étudier s'il y a lieu d'apporter ultérieurement des améliorations au système et d'arrêter pour l'avenir un ordre de priorité, et enfin il fournit une justification indépendante des frais engagés pour la mise au point.

5.7 Entretien du système

5.7.1 Motifs de l'entretien

Rien n'est permanent, y compris les ordinateurs et les systèmes informatiques. Dès l'entrée en service, des changements s'imposent. Les motifs peuvent en être les suivants :

- Les défauts non décelés antérieurement sont inévitables. Même lorsqu'un système fonctionne normalement depuis un certain nombre d'années, l'absence de défaut n'est aucunement garantie. Il est possible que le concours de circonstances qui mette le défaut en évidence ne se soit pas encore produit. Les routines de fin d'année peuvent comporter un défaut qui ne se manifestera que dans 12 mois.

Dans un nouveau système, les défauts se manifestent inévitablement au cours des premiers cycles.

- Après avoir exploité et observé le système en grandeur réelle à plusieurs reprises, les responsables du système et l'opérateur sur ordinateur peuvent être en mesure de suggérer des changements propres à accélérer les opérations et à en réduire le coût. L'usager constatera éventuellement que certaines formules et procédures peuvent être améliorées compte tenu de l'expérience acquise de façon à en faciliter l'utilisation.
- Le changement le plus radical est l'acquisition d'un ordinateur nouveau et différent; tout le système doit alors être réécrit. Mais il s'agira le plus souvent d'un nouveau type de périphérique ou d'une nouvelle caractéristique apportée au logiciel, et il est logique de modifier le système pour en tirer parti.
- Modification du volume des transactions à traiter, en excédent par rapport aux prévisions. Cette évolution peut appeler une amélioration du matériel.
- Modifications législatives, par exemple, modifications du taux des droits, changements tarifaires - l'adoption du Système harmonisé amènera de profonds changements dans les systèmes actuels - nouvelle politique commerciale (contingents, restrictions), nouvelles taxes, par exemple, TVA, etc., à l'importation.
- Mise en oeuvre de systèmes connexes, par exemple, si une administration dispose d'un système de traitement des déclarations déjà en service et souhaite désormais adopter un système de contrôle des cargaisons, la conception du premier système devra être partiellement modifiée de façon à constituer une interface avec le nouveau système de contrôle des cargaisons.

5.7.2 Types d'entretien

Les travaux d'entretien des systèmes peuvent se répartir en quasi-totalité entre les catégories suivantes :

- Modifications (urgentes ou non) qui n'appellent aucun changement majeur à la logique du système.
- Révisions qui appellent une nouvelle conception et une nouvelle programmation, par exemple, changements apportés aux spécifications d'entrée ou de sortie - nouvelles formules de saisie, nouveaux états requis.

Refonte de la mise au point appelant une nouvelle conception du système ainsi qu'une programmation et des essais de grande envergure, par exemple, changements majeurs apportés à la logique du traitement compte tenu des nouveaux besoins exprimés. Il ne s'agit peut-être pas ici d'une question d' « entretien » puisque la refonte de la mise au point doit reprendre toutes les phases comme s'il s'agissait d'un nouveau projet (de l'étude de faisabilité jusqu'à la mise en oeuvre).

Toutefois, même les modifications mineures apportées au système doivent faire l'objet d'essais approfondis avant la mise en exploitation.

5.7.3 Responsabilité de l'entretien

Lorsque les systèmes douaniers sont mis au point par des consultants externes, le contrat doit préciser l'entretien à assurer, au moins à court terme. Le personnel de la douane (appartenant au service de l'informatique) doit collaborer étroitement avec les consultants au cours de la mise au point du projet pour acquérir la certitude qu'il est entièrement familiarisé avec tous les aspects du système. Le service informatique sera alors chargé de l'entretien courant.

En cas de modification plus approfondie, il pourra s'avérer nécessaire d'engager à nouveau des consultants externes; si le service informatique dispose de l'expérience et des effectifs suffisants, il pourra entreprendre lui-même ce travail.

Lorsque les systèmes mis au point au sein de l'administration, le service informatique dispose généralement des connaissances et de l'expérience suffisantes pour maintenir le système qu'il a lui-même mis au point.

5.8 Installation d'un Service d'Assistance

5.8.1 Engagement de service auprès des usagers de la douane

L'idée de mettre en place un service d'assistance découle d'un engagement à servir les usagers. La douane doit déclarer son engagement de service, tout en restant consciente des limites de ses systèmes. Certaines administrations publient leurs engagements de service dans des Chartes destinées aux usagers.

Qui sont les usagers de la douane ? Il est relativement facile d'identifier les usagers de la douane. Les importateurs, exportateurs, agents en douane, voyageurs et responsables d'entrepôts, transporteurs etc. sont les premiers usagers qui viennent à l'esprit. Cependant, une approche rigoureuse vise à identifier toutes les parties qui interagissent avec la douane.

Exigences du service et modes de prestation : la définition des besoins du service s'effectue tout d'abord sur le tableau, lors de la conception des services. Certains des protagonistes dans les schémas de cas d'utilisation sont les bénéficiaires du service et d'autres en sont les prestataires. Les besoins du service aux usagers et les moyens correspondants pour remplir ces exigences peuvent figurer parmi les spécifications du cas d'utilisation.

Par exemple, les importateurs, exportateurs et leurs agents recherchent des renseignements sur la logistique d'un chargement, la mainlevée ou encore d'autres renseignements commerciaux (exigence de service) et souhaitent obtenir ces renseignements par voie électronique (mode de prestation du service).

Domaines de service et demandes de service : la douane sert un nombre important d'usagers et doit de même assumer des responsabilités considérables. Il est donc nécessaire de distinguer différents domaines de service. A chacun de ces domaines de service correspondra une liste habituelle de 'Demandes de service', qui seront réparties parmi un certain nombre de personnes appelées à traiter ces demandes. Voici quelques exemples qui illustreront cette situation :

L'importation, l'exportation, et le transit peuvent être considérés comme des domaines de service différents et tout retard ou problème survenant en rapport avec une demande de drawback serait une demande de service.

L'infrastructure informatique est généralement complétée d'un service d'assistance. Cette infrastructure entre en jeu pour garantir qu'un cycle de prestation de service est parvenu à son terme (par exemple, à travers l'émission d'un avis de mainlevée, faisant suite à la déclaration d'un usager). L'ensemble de cette infrastructure peut être divisé en domaines de service et, à chacun de ces domaines, on peut faire correspondre une demande de service.

Normes de service et engagements de service : Il est relativement aisé d'identifier les exigences du service lorsque les normes correspondant à ce service sont connues et établies. Les normes de service répondent généralement aux attentes des usagers. Elles consistent le plus souvent en paramètres mesurables de l'offre de service – comme le temps d'attente pour l'examen d'un document ou le délai nécessaire pour un remboursement. D'autres normes de service sont intangibles – comme par exemple la qualité des renseignements fournis sur le site Web ou l'amabilité de l'inspecteur de la douane. Toutefois, toutes les normes de service correspondent à des comportements mesurables d'un individu, d'un groupe et de systèmes. On considère souvent que ce sont les normes de service qui président à la conception des systèmes. L'inverse est également vrai. Les systèmes en place peuvent limiter les capacités de la douane à répondre de manière appropriée. Par exemple, une procédure manuelle ne peut autoriser une prestation de service aussi rapide qu'un système informatisé.

5.8.2 La douane a-t'elle besoin d'un service d'assistance?

Tout modèle d'organisation qui ambitionne d'assurer une prestation de services à distance doit pouvoir s'appuyer sur un service de soutien à distance. Avec l'introduction de la TI dans la douane, le besoin d'un service d'assistance se fait sentir pour la plupart des administrations des douanes. Le type de service d'assistance adopté (taille et caractéristiques des services rendus) est déterminé par les estimations du niveau des demandes de service et des plaintes. Habituellement, il est facile de procéder à une estimation par catégorie des besoins d'un service destiné aux usagers. Il est toutefois apprécié que les niveaux de service assurés aient une incidence sur le respect des règles par les usagers. Les services d'assistance sont-ils à même de renforcer l'efficacité d'une prestation de service ? Assurément, un service d'assistance efficace modifierait la perception par l'usager des services offerts.

Compte tenu de la position de monopole que détient la douane, les questions liées à la préservation des activités ne se posent pas (à la différence des autres organisations commerciales). Les usagers ne peuvent pas être récupérés par la concurrence. L'efficacité de la douane pourrait cependant permettre de renforcer la productivité de nos usagers et d'améliorer la confiance des entreprises vis-à-vis de l'environnement opérationnel. Si un élément du dispositif ou une partie du réseau devenait inopérant, cela pourrait entraîner une perte de productivité. Le service d'assistance pourrait officiellement dépister le défaut en cause afin d'améliorer la productivité d'un actif donné, que ce soit pour les usagers internes ou externes.

5.8.3 Les différents aspects d'un Service d'Assistance

5.8.3.1 Le Service d'Assistance, au contact avec les usagers :

Les termes 'service d'assistance' renvoient au concept d'une interface unique, dans une organisation, chargée de gérer les demandes de service. Tout service comporte le plus souvent une partie opérationnelle 'en première ligne' et une autre partie, agissant 'en coulisses'. Cette dernière consiste le plus souvent en un réseau complexe d'opérations liées à la création et à la prestation de services, échappant habituellement aux regards des usagers internes ou externes. Pour les usagers, la consommation de services doit être une expérience agréable, apportant toute satisfaction. Le service d'assistance, qui représente pour l'usager le premier contact humain, se trouve à cet égard en première ligne pour enregistrer les demandes de l'usager et les convertir en problèmes d'ordre technique et commercial, appelant une résolution. Ensuite, le service d'assistance recherche la solution au problème posé en faisant appel à la partie opérationnelle non apparente, qui aura pour mission de répondre à la demande formulée, et communique cette réponse à l'usager dans un langage qui lui sera compréhensible. L'assistance est productive si elle est en mesure de résoudre un problème et de satisfaire la demande de l'usager. Le service d'assistance est une facette amicale d'une organisation, permettant d'étendre le champ d'application des principales procédures de cette organisation. D'une certaine manière, il est un centre de communication et de transfert de compétences.

5.8.3.2 Contacts avec le service et 'moments de vérité' :

La douane, de par ses fonctions de collecte des impôts et d'application des lois n'est pas spécialement destinée à faire plaisir aux usagers. Toutefois, les différents points de contact avec les usagers, lors d'opérations quotidiennes, constituent pour la douane autant de 'moments de vérité'. Ces 'moments de vérité' représentent pour l'usager son unique expérience du service. C'est au personnel du service d'assistance qu'il revient d'assurer la production et le contrôle de cette expérience du service par l'usager et du niveau de satisfaction résultant du contact avec le service.

5.8.3.3 Restauration du service

De fait, lorsque la douane met en place des systèmes informatiques permettant l'accès à distance de ses services par les milieux commerciaux et les utilisateurs internes, le service d'assistance est l'unique recours en cas de problème. Dans l'hypothèse d'une défaillance de service, le service d'assistance n'est généralement pas en mesure de gérer ce genre de situation et il revient alors au responsable d'intervenir pour mettre en œuvre les opérations de contrôle des dégâts occasionnés ou de restauration du service.

5.8.4 Le Service d'Assistance en tant que porteur de valeur

Si le service d'assistance est de nature intangible, sa valeur aux fins de la prestation de services douaniers est bien souvent tout aussi immatérielle. Il est en effet difficile de mesurer cette valeur mais l'action d'un service d'assistance peut être mise en relation avec des facteurs mesurables tels que 1) la continuité des activités, 2) les plaintes 3) les préférences affichées pour les options de service 4) les améliorations des cycles de durée 5) les pertes de productivité imputables à des questions d'ordre technique.

L'efficacité du service d'assistance est indissociable de l'image d'efficacité que donne la douane. Les procédures et fonctions liées au service d'assistance mais qui font partie intégrante de la prestation de service sont les suivantes :

- Service d'assistance et site Web sont complémentaires : l'utilisation de plus en plus large d'Internet en tant que moyen de communication a conduit la douane à en faire son outil de prédilection pour développer l'information aux usagers. C'est un outil asynchrone, permettant aux usagers d'y recourir quand ils le souhaitent sans avoir à s'adresser à quiconque. Les opérations et les procédures du service d'assistance devraient constituer un complément du site Web et faire partie des outils de communication, au même titre que les contenus Web ou d'autres éléments du plan de communication et de publicité. Le service d'assistance est souvent le dernier rempart d'une stratégie de prestation de services mais peut, de manière permanente, s'ajouter aux QFP et autres didacticiels inclus dans l'offre de service.
- Auto-apprentissage des usagers : très souvent, les administrations des douanes ont dû surmonter des difficultés lors de l'introduction de nouveaux services à distance comme ceux permettant d'échanger des données par voie électronique ou de remplir un dossier à distance. Quels que soient le type de formation dispensée ou les ateliers organisés pour former les usagers, le lancement de ces nouveaux services sera toujours une source d'erreur entraînant des défaillances de service. L'auto-apprentissage des usagers se déroule suivant des cycles permanents de formation et d'amélioration. Il constitue un objectif et le service d'assistance fait partie intégrante de cette stratégie.
- Gestion des changements : Les services d'assistance peuvent jouer un rôle de premier plan en matière de gestion du changement. Les conseils sur les procédures technologiques et commerciales, dans un environnement changeant, constituent un défi qu'il importe de relever. Lorsqu'il devient indispensable de développer des nouvelles technologies ou procédures commerciales, les membres du personnel du service d'assistance sont des pièces essentielles de la planification stratégique et du programme général d'assistance aux usagers. Le service d'assistance peut, en anticipant les éventuels problèmes, réduire les risques liés au lancement d'un service, même si seuls les services testés sont mis en oeuvre. Il joue un rôle vital pour construire et tester les nouveaux services ainsi que lors du "passage à la production". Il peut faire état de carences survenues d'un bout à l'autre d'un service donné.
- Gestion des connaissances : Le service d'assistance est à la fois un dispositif permettant l'acquisition de connaissances et le test de solutions nouvelles. Si une question du type "Quelles sont les trois principales sources d'irritation auxquelles l'utilisateur est confronté ?" est posée au service d'assistance, les problèmes rencontrés par les services seront immédiatement identifiés. Le dispositif de gestion des appels est en mesure de gérer le nombre et le niveau des appels pour différents services. Les demandes peuvent être classées par catégories et les "solutions qui marchent" peuvent être décrites dans la base de données du service d'assistance. Ainsi, grâce à un accès direct aux solutions de la base de connaissances, les agents du service d'assistance et les usagers gagnent du temps.
- Gestion des niveaux de service : Le service d'assistance est une composante essentielle pour l'établissement de rapports sur les niveaux de service assurés, mais il fonctionne souvent conjointement avec d'autres outils et sources de

renseignement sur les interruptions de service. Des outils informatiques sont fréquemment mis en place pour contrôler la disponibilité des dispositifs, services et procédures de TIC. Ils se révèlent très pratiques pour regrouper les données qui permettront de livrer un tableau d'ensemble du niveau des services assuré.

5.8.5 Comment mettre en place un Service d'Assistance?

Cinq éléments sont nécessaires à la mise en place d'un service d'assistance :

(1) **La TI :** le lancement d'un service d'assistance requiert la mise en œuvre d'éléments de la TI. Ces éléments permettent aux agents du service d'assistance d'accéder rapidement aux renseignements pertinents aux fins du traitement des demandes. Aujourd'hui, la plupart des composants logiciels et matériels autorisent un contrôle à distance. De plus, il convient de disposer de lignes téléphoniques assurant une réponse interactive aux usagers, et complétées par un agent susceptible de prendre en charge les communications. Un certain nombre de solutions existent, qui assurent un acheminement approprié des appels et la gestion du volume des appels et qui garantissent la productivité des agents du service d'assistance chargés d'y répondre. Ces solutions consistent en un mélange d'éléments matériels et logiciels. Pour plus d'efficacité, les demandes doivent être consignées, résolues et contrôlées.

(2) **L'élément humain :** les personnes assurant un service d'assistance sont des employés susceptibles d'entrer en contact avec les usagers pour fournir des renseignements et des services. Ces ressources peuvent provenir de l'organisation elle-même ou d'un processus d'externalisation.

(3) **Les connaissances** : les renseignements relatifs aux procédures essentielles participant aux cycles de prestation des services doivent pouvoir être accessibles à distance par le service d'assistance. Les incidents susceptibles d'entraîner des dysfonctionnements de service doivent être reportés sur des diagrammes cause-effet (diagrammes *Ishikawa)* et toutes les causes des dysfonctionnements du service provenant de problèmes liés à l'équipement ou aux logiciels doivent être contrôlées et revues à distance par le service d'assistance. Sur une période donnée, les cycles de résolution des demandes conduisent à la création d'une base de données regroupant toutes les solutions qui marchent et pouvant être mises en œuvre pour des incidents de même nature.

(4) **Un modèle de service d'assistance** : un agent du service d'assistance a souvent tendance à se défausser d'un problème en le renvoyant à un autre service. Le modèle de service d'assistance doit donc s'appuyer sur le principe de service suivant : les utilisateurs doivent avoir un seul correspondant qui comprenne à la fois quels sont les besoins de l'usager et quels sont les objectifs de service (lesquels doivent être précisés). L'usager peut avoir un problème lié à son activité ou un problème de communication. Dans les deux cas, le service d'assistance devra pouvoir y répondre grâce à un menu de réponses prédéfinies, des scénarios d'interaction et des tableaux de réponses hiérarchisées.

5.8.6 Comment évaluer un Service d'Assistance ?

La performance du service d'assistance est très difficile à évaluer car il porte sur des événements intangibles et passagers, survenant lors d'une prestation de service à distance. Cependant, nous devons évaluer le degré de réussite des services d'assistance. Des critères objectifs basés sur les résultats doivent être élaborés afin de pouvoir juger du succès du service d'assistance, comme dans le tableau qui suit :

	CRITERE	**MODE D'EVALUATION**
1.	Crédibilité, sincérité et politesse	Enquêtes auprès des usagers
2.	Délai de réponse	Echantillonnage d'appels, acheminement et

	CRITERE	MODE D'EVALUATION
		contrôle des appels
3.	Délai de résolution	➢ Nombre d'appels/d'incidents ➢ Nombre de résolutions ➢ Durée des appels ➢ Nombre d'usagers pris en charge ➢ Nombre brut de résolutions lors du premier contact ➢ A partir des indications temporelles des bases de données sur la gestion et la consignation des appels.
4.	Durée des appels par comparaison à la durée passée sans appel	Voir ci-dessus
5.	Utilisation efficace des possibilités de formation des usagers	➢ Rapport des agents chargés des appels ➢ Enquêtes auprès des usagers
6.	Promotion de l'auto-apprentissage des usagers	Nombre de QFP; diminution des appels sur un sujet.

5.8.7 Incidence du Service d'Assistance sur le fonctionnement de la douane

Il est nécessaire d'intégrer les programmes d'assistance aux usagers au service d'assistance car l'information des usagers est de nature à favoriser et à renforcer le respect spontané des dispositions. Un service professionnel et structuré de soutien aux usagers peut permettre d'améliorer le niveau d'application des dispositions, tout simplement en facilitant considérablement le respect de ces dispositions par les usagers. Les usagers savent alors que quelqu'un est à leur écoute. Grâce à la technologie moderne, l'usager dispose de tous les renseignements nécessaires sur son bureau mais, dans la réalité, les gens veulent pouvoir communiquer avec d'autres êtres humains, capables de faire preuve d'empathie et de résoudre leurs problèmes. Le concept de service d'assistance découle toujours d'un besoin d'amélioration du soutien et, par là, il peut constituer l'avant-garde d'une gestion des changements.

6. APERCU DES PRINCIPAUX DOMAINES D'APPLICATION

(Norme 7.1)

6.1 Introduction

L'introduction des TIC peut présenter des avantages pour la douane dans de nombreux domaines. Cette partie décrit les principales pratiques, procédures et formalités douanières sur lesquelles la TI peut avoir une incidence très sensible. En outre, la douane peut travailler en étroite collaboration avec d'autres organismes chargés de la réglementation des flux transfrontières en vue du développement d'une solution de Guichet unique. (Veuillez consulter le Recueil de l'OMD intitulé "Comment construire un environnement de Guichet unique"). Les principaux domaines fonctionnels sont les suivants :

- contrôle d'inventaire des cargaisons ;
- traitement des déclarations de marchandises (à l'importation et à l'exportation, en transit, pour perfectionnement actif, etc.) et notamment le traitement avant l'arrivée/le départ des marchandises ;
- gestion des licences, permis, certificats et autres types d'autorisation
- notification de la mainlevée ;
- lutte contre la fraude douanière ;
- sélection (notamment évaluation des risques et ciblage) ;
- contrôle préalable des voyageurs ;
- comptabilité des recettes ;
- statistiques du commerce extérieur ;
- systèmes intégrés de gestion (SIG) ;
- établissement des rapports ;
- stockage des données ;
- enregistrement des partenaires commerciaux et gestions des programmes d'Opérateurs économiques agréés (OEA)
- Bureautique ;
- Intranet et extranet en milieu douanier.

Idéalement, un système informatique douanier global doit pouvoir assurer l'ensemble de ces fonctions. Certains pays ont déjà mis en place des systèmes globaux de cette nature. De nombreux autres n'ont informatisé que certaines de ces opérations ou ne les ont informatisées que dans un nombre réduit de ports, aéroports, etc. Nombre des applications énumérées ont une incidence sur d'autres applications. Par exemple, les données saisies dans la déclaration de marchandises dans le cadre d'un système de traitement des déclarations peuvent être exploitées par un système de comptabilisation des recettes pour établir les comptes des déclarants et par un système d'établissement des statistiques du commerce extérieur. De même, les renseignements stockés dans un système concernant la lutte contre la fraude peuvent être utilisés dans le cadre d'un système de contrôle d'inventaire des cargaisons, de traitement des déclarations de marchandises ou de contrôle des voyageurs aux fins du contrôle douanier. Dans de nombreux cas, le matériel (unités

centrales, terminaux à écrans de visualisation, imprimantes, réseaux de télécommunication) et les fichiers informatiques sont communs à plusieurs systèmes.

Il n'est parfois ni possible ni pratique de concevoir un système de TI global couvrant l'ensemble des procédures et des pratiques de la douane. Toutefois, lors de la conception d'un système, tous les aspects doivent être pris en compte, y compris les procédures, les bases de données, l'interaction entre les différentes procédures et les données. Le système doit être conçu de façon modulaire ; cela permet d'en concevoir des parties distinctes à différents moments et de les intégrer en cas de besoin à d'autres parties ou d'autres systèmes.

Quelle que soit l'application choisie pour le lancement d'un système de TIC, il convient de s'assurer que les normes de données internationales sont utilisées. A cet égard, le Modèle de données de l'OMD constitue la ressource la plus utile. [Veuillez consulter la "Recommandation du Conseil de coopération douanière concernant l'utilisation du Modèle de données de l'OMD".]

6.2 Validation des données

Les systèmes informatiques doivent permettre :

- de déceler et de signaler les erreurs les plus graves; et
- de déceler et de signaler les erreurs potentielles (en appliquant donc certains critères de jugement aux données).
- Les erreurs peuvent être détectées à deux moments différents :
- en premier lieu, au moment de l'introduction. Cette étape est parfois désignée sous le nom de validation des données et traite généralement des erreurs absolues; et
- en second lieu, lors de la mise à jour. Cette opération permet non seulement de déceler les erreurs absolues mais également d'effectuer des contrôles de vraisemblance en comparant les renseignements à ceux provenant d'un fichier maître.

Il est possible de combiner les deux étapes ci-dessus si les fichiers maîtres sont accessibles en ligne lors de la saisie des données. Les vérifications habituellement réalisées au moment de la saisie des données sont les suivantes :

Type	**Explication**	**Exemples**
Présence des champs requis	Vérifie que tous les champs nécessaires ou obligatoires sont présents. Cette vérification est particulièrement importante s'il existe des champs facultatifs pouvant devenir obligatoires lorsque d'autres renseignements facultatifs sont communiqués.	Le "numéro de l'opérateur commercial" doit être indiqué si un paiement différé est sollicité.
Nombre de caractères	Vérifie que les champs contiennent le nombre de caractères requis.	Si le champ "code tarifaire" contient un nombre fixe de 8 caractères, les renseignements indiqués dans ce champ qui ne comportent pas 8 caractères

Type	Explication	Exemples
		seront rejetés.
Contrôle de la conformité	Vérifie que les nombres ou codes sont conformes à la liste des codes prescrite	Si la fourchette 7000 - 7999 est allouée à une liste de codes, tout nombre situé en dehors de cette fourchette sera rejeté. Le pays d'origine doit être indiqué au moyen des codes de pays de la norme ISO 3166
Vérification des caractères	Vérifie que les champs contiennent le type de caractère prévu;	Si la donnée "pays d'origine" se présente sous la forme d'un code alpha à 2 caractères, les données seront rejetées si des caractères numériques sont décelés.
Chiffres de contrôle	Il s'agit d'un chiffre d'auto-contrôle créé au moyen d'une formule mathématique ou d'un algorithme. Il est utilisé pour repérer les nombres faux ou comportant des erreurs de transcription ou de transposition.	La validité du numéro d'enregistrement d'un opérateur commercial peut être vérifiée en le soumettant au même calcul que celui ayant permis d'obtenir le chiffre de contrôle original.
Vraisemblance	Vérifie, avant tout traitement, si les quantités sont anormalement élevées ou faibles	Est-il vraisemblable qu'un super pétrolier transportant du pétrole brut déclare 100 tonnes ?

Les vérifications peuvent être réalisées lors d'une mise à jour, comme suit :

Nouveaux enregistrements	Lorsqu'un nouvel enregistrement complet est mémorisé dans le fichier maître, une procédure de vérification permet d'éviter les doubles emplois.
Enregistrements supprimés	Lorsqu'il est indiqué qu'un enregistrement doit être effacé, une procédure de vérification permet de déterminer si l'enregistrement existe. S'il n'existe pas, une erreur est signalée.
Cohérence	Lorsqu'un fichier maître est modifié, il convient de s'assurer que les nouvelles données sont cohérentes par rapport à celles figurant déjà dans le fichier maître. Par exemple, lorsque le fichier maître sur les salaires est mis à jour en incorporant les paiements d'heures supplémentaires, il faut vérifier si les employés sont fondés à bénéficier de tels paiements.

D'autres vérifications, dénommées contrôles de vraisemblance, qui font appel à des paramètres prédéterminés, servent à évaluer la qualité des renseignements introduits s'agit généralement de comparaisons destinées à repérer les données incompatibles (par exemple, un navire venant de New York est peu susceptible de décharger sa cargaison à Heathrow; le prix d'une marchandise déterminée venant d'un pays particulier est inférieur au prix escompté, etc.).

Lorsqu'une erreur est décelée, les mesures généralement prises sont les suivantes. Lors de la saisie dans le système, les erreurs provoquent le rejet de la donnée qui devra être corrigée puis saisie à nouveau. Les contrôles de vraisemblance permettent en général de poursuivre l'opération mais signalent la situation pour vérification ultérieure avant l'acceptation ou le rejet définitif. Un sous-système de contrôle automatique peut également être installé garantissant que les erreurs signalées soient traitées dans un délai déterminé. Le système peut également rejeter ou accepter automatiquement toute erreur signalée non traitée dans le délai prévu et dresser ensuite l'inventaire des erreurs en précisant la solution apportée.

Une validation appropriée des données garantit la qualité de ces données. Les informations ci-dessus laissent à penser que la validation des données est en grande partie influencée par les "types de données" utilisés pour représenter les informations. Le Modèle de données de l'OMD permet une utilisation maximale des codes et identificateurs, et il dissuade de recourir à des champs de "texte libre", ce qui entraîne une amélioration de la qualité des données.

6.3 Contrôle d'inventaire des cargaisons

Le contrôle des cargaisons entre leur arrivée, le paiement des droits ou la constitution d'une garantie et le dédouanement pose de nombreux problèmes aux administrations. La douane doit veiller à ce qu'il soit convenablement rendu compte de toutes les marchandises arrivées sur son territoire. La comparaison manuelle des relevés sur papier est une tâche très lourde, génératrice d'erreurs et coûteuse en main d'œuvre. Un système informatique de contrôle des cargaisons permet de confronter automatiquement les renseignements figurant sur les manifestes et ceux figurant sur la déclaration en douane. Des modifications peuvent être apportées aux données afin d'enregistrer les marchandises excédentaires ou manquantes après vérification de l'envoi par la douane. Les données peuvent être préalablement soumises à des critères de sélectivité déterminés pour signaler aux fonctionnaires des douanes les envois à haut risque. Après présentation de la déclaration correspondant aux marchandises en question, l'ordinateur apure automatiquement l'enregistrement d'inventaire ou signale une anomalie pour suite à donner. Des relevés répertoriant les marchandises non déclarées dans les délais prévus sont également produits pour complément d'enquête.

Dans certains cas, la douane ne dispose pas de son propre système informatique de contrôle d'inventaire mais s'appuie sur les systèmes informatiques des transporteurs, des autorités portuaires, etc. Elle contrôle ces systèmes par des audits. Cette solution peut s'avérer très rentable pour la douane, notamment dans la mesure où la plupart des transporteurs et des autorités portuaires se sont informatisés.

La saisie dans le système douanier de renseignements concernant le manifeste avant l'arrivée des marchandises permet à la douane de procéder à une évaluation initiale du risque que présentent les envois. Le plus souvent, lorsque les marchandises sont de faible valeur ou ne font l'objet d'aucune restriction, aucune évaluation ultérieure n'est nécessaire.

6.4 Traitement des déclarations de marchandises (à l'importation et à l'exportation), et notamment traitement avant l'arrivée/le départ des marchandises

(Normes transitoires 3.18 et 3.21)

Le traitement des déclarations de marchandises importées ou exportées est l'une des principales tâches qui incombent à toute administration des douanes. Il n'est donc pas surprenant que de nombreuses administrations aient obtenu d'importants gains de productivité en informatisant cette procédure.

La saisie des renseignements peut s'effectuer de diverses manières, comme suit :

- saisie des données par les fonctionnaires des douanes ;
- introduction directe des données, soit par les entreprises, soit par l'intermédiaire de bureaux de services; et/ou
- lecture des codes barres, dispositifs d'auto-identification et de reconnaissance optique des caractères (ROC)
- Autres capteurs et dispositifs de géolocalisation
- transmission des données.

Lorsque les données figurant sur la déclaration de marchandises ont été introduites dans le système informatique, elles sont soumises à un certain nombre d'opérations, dont les principales sont les suivantes :

- validation des données (voir 6.2 ci-dessus) ;
- classement et origine ;
- évaluation des risques et la sélectivité
- vérification de la valeur ;
- liquidation des droits; et;
- recouvrement des droits (droits de douane, T.V.A., droits d'accises, etc.)

La mise en œuvre d'une base de données tarifaire intégrée permettra de déterminer avec rapidité et exactitude les préférences et les restrictions éventuellement liées à la déclaration, afin de garantir l'application des taux de droits corrects.

L'évaluation correcte des marchandises, y compris des mesures prises à l'échelon national et international est une condition préalable de la liquidation correcte des droits. Une base de données concernant l'évaluation peut être utilisée pour identifier les valeurs acceptables pour des marchandises déterminées provenant de certains pays. La base de données peut aussi appeler l'attention sur les valeurs se situant en dehors des fourchettes acceptables.

Lorsque les droits ont été liquidés (et les devises converties, le cas échéant), les renseignements peuvent être transmis au système de comptabilisation de recettes.

Au cours de ces opérations, l'usager est informé des erreurs éventuelles par un message affiché sur l'écran et peut alors procéder à des rectifications. Il est également informé des documents justificatifs exigés le cas échéant pour le dédouanement des marchandises, par exemple, licences, certificats d'origine, etc. La douane pourrait, plutôt

que de demander des copies sur support papier des documents justificatifs, procéder à une vérification en ligne des informations contenues dans les documents justificatifs. Si cela n'est pas possible, les documents justificatifs peuvent être reçus par voie électronique à des fins de vérification automatique. (Veuillez consulter la Recommandation de l'OMD concernant la dématérialisation des documents justificatifs).

Une fois les formalités remplies, le système peut également produire le bon d'enlèvement (voir également le paragraphe 6.6). Lorsque le contrôle d'inventaire des cargaisons est également informatisé, un rapprochement est généralement établi entre les données concernant la cargaison et celles qui figurent sur la déclaration de marchandises, l'inventaire est ensuite apuré.

Les systèmes de traitement des déclarations de marchandises peuvent également produire à l'intention des entreprises des relevés périodiques répertoriant les montants dus au titre du système du paiement différé, afin d'assurer le transfert électronique des fonds entre les comptes de l'opérateur commercial et la douane.

La possibilité de recevoir les renseignements de la déclaration en douane avant l'arrivée ou le départ des marchandises permet à la douane de procéder aux formalités requises, y compris la liquidation des droits, préalablement à l'arrivée matérielle des marchandises sur le territoire douanier. En cas d'exportation, il s'agit des marchandises qui quittent le territoire douanier. Les erreurs peuvent le cas échéant être signalées à l'avance à l'entreprise; les rectifications nécessaires peuvent alors être apportées, ce qui réduit les retards éventuels dans les formalités de mainlevée.

6.4.1 Traitement avant l'arrivée/le départ des marchandises

Les renseignements de la déclaration en douane communiqués avant l'arrivée des marchandises ou avant leur départ sont traités de la même manière que la déclaration de marchandises comme décrit dans la section 6.4. L'information reçue à l'avance de l'arrivée des marchandises aide les douanes à prendre les décisions relatives à la recevabilité et le dédouanement des marchandises.

6.4.2 Gestion des licences, permis, certificats et autres types d'autorisations

L'importation et l'exportation de certaines marchandises sont soumises à une réglementation. Afin d'appliquer et de gérer ces restrictions, les autorités délivrent des licences, des permis, des certificats, etc. Ces documents contiennent une description des marchandises concernées et précisent quelles sont les catégories, la quantité et la valeur des marchandises susceptibles d'être importées ou exportées. Les procédures liées au cycle de vie des licences, permis, certificats et autres types d'autorisations peuvent être gérées efficacement grâce aux systèmes de TIC. Ces procédures comprennent l'émission, l'utilisation, l'annulation et l'expiration des diverses autorisations. La manipulation par voie électronique des renseignements contenus dans ces types de documents contribue à améliorer la gestion des contrôles transfrontières et notamment des restrictions non tarifaires. Cette application est particulièrement importante dans le contexte d'une approche de Guichet unique, où plusieurs autres organismes de réglementation des flux transfrontières sont chargés de gérer le cycle de vie des licences, permis, certificats et autres types d'autorisations.

6.5 Rapprochement des renseignements

Le rapprochement ou la confrontation automatisée des renseignements, par exemple de ceux contenus dans les systèmes de contrôle d'inventaire et de traitement des déclarations en douane, constitue l'une des principales opérations réalisées par la douane. Tout écart entre les renseignements confrontés est mis en évidence, et le système établit un rapport de sous/surévaluation.

Les techniques informatiques de rapprochement des renseignements peuvent également être appliquées au régime douanier de l'admission temporaire avec réexportation en l'état.

Dans le cadre de l'informatisation des systèmes de comptabilisation des recettes, les droits dus, extraits des renseignements figurant sur la déclaration de marchandises, peuvent être confrontés aux relevés de manière à produire en temps voulu des renseignements comptables précis. Ce système de comptabilisation peut également être utilisé pour valider les demandes de drawback.

6.6 Notification de la mainlevée

(Norme transitoire 6.9)

Bien que le traitement des déclarations de marchandises constitue le domaine d'application de la TI par excellence, la notification électronique de la mainlevée peut être abordée séparément. L'établissement d'interfaces avec les systèmes automatiques de mainlevées existantes et la saisie de la mainlevée pour diffusion auprès d'une ou de plusieurs entreprises au moyen d'Internet ou du courrier électronique peuvent présenter de nombreux avantages. Un système électronique de notification de la mainlevée peut être installé même si toutes les transactions sont traitées sur la base de documents imprimés. Les notifications électroniques de mainlevée peuvent aussi être communiquées par le biais d'un accord approprié avec les opérateurs d'entrepôt qui assurent la garde matérielle des marchandises. La diffusion en temps voulu des notifications électroniques de mainlevée peut présenter des avantages pour la douane ainsi que pour les entreprises, notamment parce qu'elle permet de réduire les délais de mainlevée.

6.7 Lutte contre la fraude douanière

(Norme transitoire 6.9)

L'avantage que présente l'utilisation des TIC pour le contrôle douanier est qu'elle permet à tous les fonctionnaires des douanes autorisés de consulter aisément les renseignements. L'informatisation permet en outre d'examiner les renseignements contenus dans les bases de données d'autres services de prévention et de répression (police, immigration, etc.). L'application des TIC permet également aux fonctionnaires des douanes de consulter de manière rapide et précise diverses données telles que critères de sélection, afin d'en apprécier l'utilité et de pouvoir ainsi réagir rapidement dans un environnement en évolution. Toutefois, il importe d'instaurer l'équilibre le plus juste possible entre, d'une part, l'application de dispositions sanctionnant les opérateurs qui enfreignent les lois et règlements en vigueur et, d'autre part, la nécessité d'offrir aux autres la plus grande transparence possible.

Pour s'assurer que la réglementation douanière est dûment respectée en utilisant au mieux les ressources limitées dont elle dispose, la douane doit recourir aux techniques de sélection et d'évaluation des risques. Bien que la mise en œuvre de ces techniques ne soit pas nécessairement liée au recours à la TI, elles ne peuvent être appliquées de manière efficace et cohérente sans celle-ci. Dans un univers informatique, des principes de sélection et d'évaluation des risques identiques peuvent être appliqués aux voyageurs et aux marchandises.

6.8 Sélection

On entend par sélection l'opération consistant à déterminer si la douane doit soumettre un envoi ou un voyageur particulier à un contrôle plus approfondi. Dans un environnement automatisé, quatre "filtres" de sélection peuvent être appliqués, à savoir, les profils internationaux, nationaux, ainsi que locaux, et les vérifications par larges épreuves. Le ciblage correspond à la partie du processus de sélection qui consiste à choisir un envoi, un voyageur, un moyen de transport, une transaction ou une entité à des fins d'examen/ de contrôle et ce, sur la base d'une analyse des risques, d'un établissement de profil, d'un examen des documents ou de techniques d'observation et d'interrogation.

Les deux premiers s'appuient sur un système de profils établis compte tenu des connaissances des fonctionnaires des douanes (à l'échelon international) et des données produites par les systèmes d'analyse des renseignements qui évaluent les risques de moins-value fiscale et d'infraction à la législation. L'intelligence artificielle et les systèmes d'experts comme les système de reconnaissance de structures types seront très utiles pour faciliter l'évaluation des risques et l'établissement de profils. (L'identification de risques ainsi que les éléments de données figurant habituellement dans les profils sont traités en détail dans la Directive de l'OMD relative au contrôle douanier).

Lorsqu'il élabore un ensemble de profils, le concepteur doit tenir compte du fait que le système doit être souple et capable de traiter des combinaisons d'éléments de données relativement complexes autant que des éléments de données isolés simples. Ces combinaisons permettent à la douane de régler finement le ciblage. A titre d'exemple, la douane pourrait souhaiter sélectionner une marchandise particulière uniquement lorsqu'elle provient d'un pays déterminé. Les appendices 2 et 3 du présent document décrivent de manière théorique un système de sélection.

La principale différence entre les profils nationaux et locaux est que les premiers doivent obligatoirement être appliqués par tous les bureaux de douane du pays, alors que les seconds ne s'imposent qu'à un nombre réduit de bureaux, voire à un seul. Toutefois, les renseignements figurant dans les profils locaux doivent être pris en considération dans l'analyse globale des risques et, le cas échéant, intégrés dans les profils nationaux. Tous les profils doivent être réexaminés à intervalles réguliers et des mesures de sécurité précisant les personnes habilitées à modifier les deux types de profils doivent être arrêtées.

Le système de sélection aléatoire repose sur un algorithme qui sélectionne au hasard les déclarations devant faire l'objet d'un examen complémentaire, par la douane.

Le système doit en outre être conçu de manière que l'interaction coordonnée entre les trois niveaux de sélection soit contrôlée, notamment pour ne pas dépasser le nombre de vérifications prévu.

Le système doit également être conçu de manière que la totalité des renseignements soit évaluée compte tenu des profils nationaux, mais que seuls les renseignements propres à telle région ou tel bureau de douane soient évalués au regard des profils nationaux et locaux, respectivement. Un dispositif permet généralement aux fonctionnaires d'encadrement autorisés de suspendre temporairement l'application d'un profil.

6.8.1 Gestion des risques

La gestion des risques conditionne étroitement l'efficacité du ciblage des envois à examiner. (Les principes à appliquer pour gérer les risques sont énoncés dans le Recueil de l'OMD sur la gestion des risques).

L'efficacité des profils de sélection dépend de la qualité des renseignements qu'ils contiennent. La révision à intervalles réguliers des profils indiquera aux fonctionnaires des douanes les éléments de données et les combinaisons d'éléments de données ayant permis de déceler des déclarations frauduleuses. L'analyse des renseignements contenus dans les déclarations proprement dites permet également de dessiner les tendances et de repérer les envois pouvant présenter des risques élevés.

"Système intégré de gestion des risques de la **Corée** *: aperçu*

La gestion des risques reposant sur la technologie de l'information et de la communication est un élément essentiel pour répondre aux défis des transactions transfrontières. La douane de la Corée (KCS) sélectionne et inspecte les voyageurs, les marchandises et les moyens de transport à haut risque sur la base des résultats d'une analyse des risques. Le KCS effectue habituellement une analyse des risques pour vérifier a posteriori les transactions illégales et les cas d'évasion fiscale, et elle a en outre mis en place en 2002un entrepôt douanier de données. Les données recueillies proviennent non seulement des services douaniers mais aussi d'autres agences gouvernementales comme le ministère de la justice, le Service national de la fiscalité, le ministère des affaires étrangères et du commerce, et le ministère des transports terrestres et des affaires maritimes. A partir de 2008, le KCS a commencé à mettre en place un Système intégré de gestion des risques assumant diverses fonctions :

- intégration et segmentation automatiques des données
- apport de renseignements personnalisé (par exemple, pour les fonctionnaires de haut rang, de rang moyen ou de terrain
- diffusion des renseignements et des critères de sélection ; et
- combinaison des facteurs de risque au moyen d'indicateurs complexes de sélection des cibles.
- (Source : Recueil 2011 de l'OMD sur la gestion des risques)

6.9 Contrôle préalable des voyageurs

Les renseignements préalables concernant les voyageurs (RPCV) permettent à la douane d'accélérer le contrôle des voyageurs. La gestion du volume croissant de voyageurs et de toute la gamme des risques existants impose de recourir aux TIC et aux renseignements préalables, afin de permettre aux agences frontalières de réaliser une évaluation des risques préalable à l'arrivée des marchandises. Les RPCV permettent de mettre en œuvre des méthodes plus efficaces et intelligentes de vérification des voyageurs et de leurs bagages. En combinaison avec d'autres renseignements, ils offrent la possibilité de procéder à des interventions ciblées. Ces interventions sont d'autant plus efficaces que la

qualité des données reçues par les agences est bonne. Le passage d'une majorité de voyageurs peut ainsi être facilité, ce qui soulage la tâche des agences aux frontières et contribue à améliorer le vécu des voyageurs.

Toutefois, pour en tirer pleinement profit et en faire un outil efficace, il faut instaurer une coopération entre les services de contrôle aux frontières (douane, police, immigration) et les transporteurs (compagnies aériennes, maritimes, etc.). A cet égard, les directives OMD/IATA/OACI concernant les RPCV précisent les renseignements maximums que la douane peut exiger et indiquent les normes à respecter dans ce domaine. Des messages normalisés internationaux ont déjà été mis au point aux fins de ces échanges.

Outre les Renseignements préalables concernant les voyageurs (RPCV), l'utilisation des données du Dossiers passagers (PNR) présente également des avantages potentiels dans le domaine de la lutte contre le trafic de drogues et autres crimes transnationaux graves. L'expression « renseignements du PNR » est l'appellation générique attribuée aux données consignées par les compagnies aériennes chaque fois qu'une passager réserve un vol. Les données du PNR contiennent des renseignements fournis par le passager et des renseignements utilisés par la compagnie aérienne à des fins opérationnelles. Les renseignements du PNR peuvent inclure des éléments d'information qui figureront également dans les RPCV. Le PNRpropose un mécanisme auquel peuvent recourir, sous un format commun, l'ensemble des différentes parties de l'industrie aéronautique (et notamment, les agents de voyage, les transporteurs aériens et les agents chargés de la manutention dans les aéroports) afin de reconnaître chaque passager et d'accéder à l'ensemble des renseignements pertinents concernant son voyage ; vol de départ et vol de retour ; correspondances (le cas échéant) et les services spéciaux exigés durant le vol.

La demande de traitement des renseignements du PNR devrait tenir compte du fait que le volume et la nature des renseignements contenus dans un PNR peuvent varier d'une compagnie aérienne à l'autre et d'un passager à l'autre, souvent en fonction du mode de réservation retenu Les éléments de données maximum qui peuvent être inclus dans le cadre des données des PNR à communiquer sont décrits dans le document 9944 de l'OACI (également dénommé *Lignes directrices sur les données des dossiers passagers (PNR).*). L'OMD, l'IATA et l'OACI ont approuvé une norme pour la transmission des données des PNR. Ce message normalisé, dénommé 'PNRGOV', et les directives pertinentes sont publiés conjointement par l'OMD, l'IATA et l'OACI.

Plusieurs Membres de l'OMD ont fait part d'utilisations réussies des RPCV et des données du PNR pour le ciblage de passagers soupçonnés d'être impliqués dans un trafic illicite de drogues ou d'autres contrebandes ou encore dans la contrebande de matières liées au terrorisme. C'est pourquoi l'OMD a adopté une Recommandation relative à l'utilisation des Renseignements préalables concernant les voyageurs (RPCV) et du Dossier passagers afin d'assurer l'efficacité des contrôles douaniers (Appendice 19).

6.10 Comptabilité des recettes

La comptabilisation des recettes est l'une des principales fonctions d'un grand nombre d'administrations des douanes. Aussi l'informatisation des procédures de comptabilisation des recettes constitue-t-elle une pierre angulaire de tout système informatique douanier intégré. Un tel système doit :

- rendre compte des droits recouvrés et remboursés et des droits ayant fait l'objet d'une exonération ou non perçus ;
- comporter un mécanisme de recouvrement et de remboursement des droits au moment du dédouanement ; et
- comporter un mécanisme permettant de différer le paiement des droits pendant un délai déterminé.

La mise en œuvre d'un système de paiement différé exige la création d'un système d'enregistrement des opérateurs commerciaux. Ce système doit contrôler l'état des garanties et calculer les recettes échues pour une période déterminée. Le paragraphe 6.13 du présent document contient de plus amples précisions à ce sujet.

Dans le cadre d'un système de comptabilité des recettes, les tâches suivantes sont particulièrement adaptées à l'application de la TI :

- contrôle informatique de la garantie constituée au titre des droits ;
- tenue des comptes de paiement différé des entreprises; et
- calcul rapide et précis des recettes.

Pour pouvoir recouvrer les droits dus lors du dédouanement, il faut que la douane accepte les espèces, les chèques, les virements bancaires, les cartes de crédit et les cartes de débit du déclarant et/ou les méthodes de paiement par transfert électronique de fonds en temps réel.

La douane doit être en mesure de rapprocher les droits effectivement recouvrés et le montant total des droits calculé par le système de traitement des déclarations de marchandises. En principe, le système devrait enregistrer le montant acquitté pour chaque transaction assorti du numéro de la déclaration en douane correspondante. Le mode de paiement doit également être enregistré. Habituellement, les montants acquittés sont ventilés par types de droits et de taxes (accises, droits de douane, taxe à l'exportation, etc.), ce qui indique aux autorités douanières le montant recouvré pour chaque catégorie.

Pour être en mesure d'accepter les cartes de paiement, la douane doit se doter des moyens techniques nécessaires pour relier les bureaux de douane au système bancaire, afin de valider les renseignements indiqués sur la carte et de veiller au versement de la totalité des montants dus.

Il existe une différence significative entre un système de paiement différé et le recouvrement des droits et taxes dus au moment du dédouanement des marchandises. Ces systèmes reposent sur la tenue d'une comptabilité individuelle pour chaque déclarant ou opérateur commercial agréé. En général, l'opérateur commercial, la douane et la banque de l'opérateur conviennent du montant maximum de droits dont le paiement est différé; ce montant est couvert par une garantie. Des renseignements détaillés concernant ce montant ainsi que chaque transaction (numéro de la déclaration en douane et montant des droits)

sont enregistrés dans une base de données reliée au système d'enregistrement des opérateurs commerciaux. Le contrôle et la gestion d'un tel système manuel mobilisent d'importantes ressources et se prêtent davantage à la fraude et aux erreurs. De même, il ne serait guère pratique de gérer un système de paiement différé manuel couvrant tout le territoire (les transactions réalisées par chaque entreprise dans tous les bureaux devant être couvertes par un seul compte). Toutefois, la mise en œuvre d'un système informatique de recouvrement des recettes facilite le fonctionnement d'un système de paiement différé à l'échelon national.

Dans un environnement informatisé, le dernier solde du compte de paiement différé est toujours accessible, alors que dans un univers manuel, cela n'est pas nécessairement le cas. En outre, dans un système manuel, il subsiste toujours un risque que le montant des droits dont le paiement est différé dépasse le montant de la garantie, ce qui expose la douane à un risque de moins-value fiscale. Un système de comptabilisation informatique des recettes empêche les entreprises de dépasser le montant de la garantie. Si le montant des droits dus pour une transaction déterminée est supérieur au solde de la garantie, le système alerte la douane.

En cas d'échange électronique de donnés, le système de la douane communique à l'opérateur commercial un message de réponse indiquant que le paiement des droits ne peut être différé faute d'un crédit suffisant. L'opérateur devrait à tout moment pouvoir solliciter des précisions concernant le solde du compte de paiement différé ou obtenir un relevé de compte.

Lorsque les droits sont échus, le montant total dû par chaque opérateur commercial agréé ainsi que les renseignements concernant son compte bancaire (numéro de compte, code de branche, etc.) doivent être communiqués à la banque concernée. A cet égard, la douane et les banques devront convenir de normes en matières d'échanges de données et de supports (EDI, bandes, disquettes, Internet) à employer. Des messages normalisés internationaux utilisables dans un environnement EDI permettent d'échanger des renseignements concernant les paiements.

6.11 Statistiques du commerce extérieur

La base de données concernant les déclarations étant la principale source de statistiques du commerce extérieur, les impératifs dans ce domaine doivent être pris en considération lors de sa conception.

6.12 Systèmes intégrés de gestion (SIG)

Une fois les données enregistrées sur un support électronique, elles peuvent être analysées à l'aide de logiciels propres à un constructeur ou de programmes "maison", selon le cas. Avant de choisir entre ces deux solutions, il est essentiel d'examiner la nature des consultations et des rapports nécessaires. Les outils d'analyse des renseignements peuvent être utilisés pour réaliser les opérations simples, comme répertorier les occurrences d'un nom, ou complexes, comme combiner des éléments de fait connexes provenant de différents fichiers, afin d'élaborer un rapport qui ne serait pas disponible par d'autres moyens.

Ces techniques sont particulièrement précieuses aux fins des enquêtes en matière de fraude et de lutte contre la fraude. Toutefois, des SIG peuvent également être utilisés par les cadres supérieurs pour s'assurer que les ressources sont utilisées efficacement. Ils permettent de faire rapport sur le nombre de déclarations traitées dans un bureau de douane déterminé, d'identifier les pics et les creux dans le volume de travail, de déterminer les types d'envois, etc.

6.13 Etablissement de rapports

Lorsqu'elles élaborent un système informatisé, les administrations des douanes doivent concevoir un moyen automatisé de produire en différé des rapports préformatés, et ce sur une base quotidienne, hebdomadaire, mensuelle ou annuelle. Il peut également s'avérer utile de concevoir un outil spécifique permettant aux fonctionnaires et au personnel d'encadrement de créer leurs propres rapports. Un système d'établissement de rapports bien conçu permet à la douane d'élaborer ses propres rapports selon les différents types de données contenus dans ses systèmes.

6.14 Gestion du cycle de vie des données

Les administrations doivent tenir compte de l'obligation légale qui leur est faite de stocker les données. Le stockage des données peut également faciliter l'établissement des rapports et servir à concevoir des outils de lutte contre la fraude et d'évaluation des risques.

Il existe de nombreux moyens de stocker des données, notamment sur des disques magnétiques tels que disques durs ainsi que sur des bandes magnétiques. Les nouvelles techniques permettent également de stocker des données sur des disques optiques (CD et DVD).

6.14.1 Recherche des données

Un système de recherche permet à la douane d'accéder en ligne aux données de nature historique. Les données qui ont été introduites ou transmises par EDI peuvent être consultées en ligne au niveau de l'en-tête/fin de fichier, du sous-en-tête et de la ligne d'entrée. Un système de recherche efficace permet à l'utilisateur de consulter toutes les versions des données introduites, la version actuelle étant affichée la première à l'écran.

6.14.2 Exploration des données

L'exploration des données peut être décrite comme une technologie du renseignement qui utilise plusieurs techniques pour rechercher des renseignements compréhensibles, utiles et dissimulés dans une masse de données stockées.

L'exploration des données permet de découvrir des tendances et des modèles cachés parmi de très nombreuses données et elle est donc très utile aux fins de l'évaluation des risques. Le produit obtenu peut prendre la forme de tendances ou de modèles implicites dans les données stockées.

6.15 Système d'enregistrement des opérateurs commerciaux

Les systèmes d'enregistrement des opérateurs commerciaux sont souvent mis au point dans le cadre d'un système de paiement différé, mais peuvent également être utilisés à

d'autres fins, par exemple, pour déterminer les facilités particulières accordées par la douane à telle ou telle entreprise. Ces systèmes contiennent habituellement des renseignements de base concernant les opérateurs commerciaux, par exemple :

- le numéro d'enregistrement de l'opérateur (qui doit si possible être le même pour tous les services) ;
- évaluation des opérateurs commerciaux
- les coordonnées de l'opérateur (nom, adresse, numéro de téléphone, etc.) ;
- les renseignements bancaires (nom de la banque, adresse, numéro de compte) ;
- le montant de la garantie (montant maximum garanti par la banque de l'opérateur) ;
- la date de débit des droits (date à laquelle le montant des droits échus doit être débité du compte bancaire de l'opérateur) ;
- les facilités douanières particulières (déclarations périodiques, entrepôts de douane, etc.) ;
- les liens avec une entreprise mère et/ou des filiales, le cas échéant.

Le déclarant sera tenu d'indiquer le numéro d'enregistrement sur chaque déclaration. Ainsi, une correspondance entre les renseignements concernant les droits et le compte de paiement différé correspondant pourra être établie, ou une mesure ou un régime douanier particulier pourra être mis en œuvre. Chaque compte doit comporter le numéro de la déclaration, la date ainsi que le montant total des droits dus pour la déclaration concernée. Le solde de la garantie doit également être tenu à jour.

Compte tenu des impératifs en matière de protection des données confidentielles, seuls les autres systèmes douaniers doivent pouvoir avoir accès aux systèmes d'enregistrement des partenaires commerciaux et doivent être strictement contrôlés (mesures de sécurité et autorisation d'accès).

6.16 Transit douanier

Le principe de base du transit douanier est de permettre aux marchandises de passer d'un bureau de douane à un autre, sur le même territoire douanier ou sur un autre territoire douanier, sans que les droits et taxes exigibles le cas échéant soient acquittés, pour autant que toutes les obligations relatives aux scellements douaniers, aux délais ou à la sécurité, etc. soient remplies.

L'échange électronique de données améliorera l'efficacité et la rentabilité du transit douanier. Il est plus facile de contrôler les mouvements en transit et en transbordement dans un environnement informatisé. Les renseignements de la déclaration peuvent être saisis à l'entrée, puis vérifiés et apurés lorsque les marchandises quittent le territoire douanier. Les contrôles de base en matière de validation et de crédibilité portent sur les données elles-mêmes et le système attribue un numéro de déclaration unique. La douane du point de départ accède aux renseignements originaux en utilisant ce numéro de déclaration unique.

L'informatisation permet d'identifier plus rapidement et plus efficacement tout mouvement en transit incomplet ou incohérent.

Le contrôle en matière de transit peut bénéficier largement de l'échange d'informations entre les administrations des douanes. Le fait de partager ces informations

en temps utile contribuera à réduire les risques de fraude tirant parti du transit. Les avantages que présente l'utilisation de la technologie de la TI dans le cadre du transit national s'appliquent également au transit international.

L'utilisation de l'EDI dans les procédures de transit connaît actuellement de nouveaux développements. Le nouveau système de transit informatisé (NCTS) de la CE et le système que conçoit actuellement l'Union internationale des transports routiers, le TIR sécurisé, en constituent deux exemples récents. La CEE/ONU a élaboré une norme électronique pour le TIR (eTIR).

6.17 Autres applications

(Normes transitoires 9.3 et 9.4)

Outre les domaines d'application déjà mentionnés, d'autres fonctions de la douane peuvent également être informatisées, par exemple :

- le remboursement des droits de douane déjà acquittés (drawback) ;
- le contrôle des contingents ;
- la gestion des amendes, pénalités, etc., douanières ;
- les renseignements tarifaires contraignants ;
- les décisions en matière de classement ;
- la mise en entrepôt, y compris la circulation des marchandises sous douane ;
- l'approbation de la déclaration (manifeste confirmé par les déclarations suivantes, déclarations concernant le transport confirmées par l'arrivée des marchandises, etc.) ; et
- les applications de gestion des ressources humaines

6.18 Bureautique

Comme toutes les administrations, la douane exerce un certain nombre de fonctions administratives. La "bureautique" vient appuyer de manière uniforme les opérations administratives générales et courantes mentionnées ci-après :

Opération de base	Opération administrative	Système d'appui
Enregistrement de lettres, de Documents, etc.	Enregistrement de renseignements Recueil de renseignements	Bases de données Logiciel de recherche
Stockage et diffusion	Archives Récupération Reproduction Traitement de textes Communication verbale Gestion de documents électroniques	Scanner/générateur de mots clés Stockage sur disque optique/base de données Recherche par mots clés sur disque optique/base de données Diffusion par courrier électronique externe, télécopie, production de disques optiques, impression automatique sur imprimantes de réseau Logiciels de traitement de textes Téléphone
Communication et planification	Diffusion des renseignements	Courrier électronique et calendrier électronique, télécopie, téléphone
Exploitation des renseignements	Analyse des renseignements Fonctions arithmétiques	Outils d'interrogation Tableur
Présentation	Présentation des renseignements	Interface graphique Progiciels intégrés

Un système de bureautique doit comprendre un ensemble équilibré d'outils choisis en fonction des besoins de l'utilisateur final. Il est important d'utiliser un système de

bureautique courant comprenant généralement au moins une interface graphique (GUI), un traitement de texte et un tableur.

Le téléphone en tant qu'instrument de la technologie de l'IC est très précieux. De plus en plus d'administrations des douanes adoptent des systèmes téléphoniques pour les aider à exécuter leurs programmes et à répondre à leurs usagers au sujet de ces derniers. Il s'agit là d'un outil technologique très utile qui peut être intégré dans un programme sans frais élevés pour une administration.

6.19 Intranet et extranet en milieu douanier

L'apparition de technologies liées à internet a également des conséquences pour la douane. En effet, celle-ci fait de plus en plus partie du réseau électronique des pouvoirs publics (e-gouvernement) en proposant tous ses services à ses usagers sur Internet. Ce réseau permet les communications internes et externes et peut faciliter grandement la diffusion des renseignements officiels au sein de l'administration et à l'extérieur. Si la solution d'un service douanier en ligne est appliquée correctement, elle est de nature à améliorer sensiblement les services rendus aux entreprises et au public. Toutefois, comme cela se vérifie lorsque l'on utilise les technologies de l'information en général, on ne peut tirer pleinement profit d'un système informatisé que si les opérations internes font l'objet d'un examen critique et sont éventuellement modifiées voire supprimées avant l'emploi de l'informatique.

Un site Internet propre à la douane auquel le public peut avoir accès, permet à l'administration de faciliter l'accès et la diffusion sur le site public des renseignements juridiques relatifs à la douane, notamment à l'intention des voyageurs et des intervenants dans le commerce international. Le site web permet également de mettre à la disposition du public ces renseignements d'une manière rentable et facilement accessible.

Un intranet à large couverture permet d'avoir accès à tous les systèmes à l'aide d'un seul et même ordinateur et de gérer de façon centralisée tous les outils et toutes les bases de données utiles. L'Intranet grâce auquel tous les renseignements et documents reçus et élaborés par l'administration sont disponibles sous forme électronique, permet de réduire la circulation des documents sur papier et leur stockage, ainsi que d'améliorer leur circulation interne.

Le Conseil de l'OMD a adopté en 1999 une Recommandation sur l'utilisation de l'Internet à des fins douanières. Il s'agit là d'un premier pas très important pour encourager les administrations des douanes à s'informatiser (voir l'appendice 10). En novembre 2003, le site web de l'OMD a établi des liens avec plus de 140 administrations douanières à l'échelon international.

7. EXTERNALISATION DES FONCTIONS DOUANIERES

7.1 Aperçu

L'externalisation intervient lorsqu'une entité achète des produits ou des services ou délègue une partie de ses fonctions à une entité extérieure, généralement spécialisée dans l'externalisation de ces produits, services ou activités, plutôt que de réaliser ces tâches en son sein même.

7.1.1 Externalisation, délocalisation et internalisation

La délocalisation est un autre terme utilisé dans le contexte de l'externalisation, lorsque l'activité qu'il a été décidé d'externaliser est réalisée dans un autre pays. L'externalisation peut intervenir dans le pays ou à l'étranger.

Toute fonction qui n'est pas une compétence de base peut être externalisée auprès d'autres entités habilitées à les réaliser. Parfois, pour éviter de perdre le contrôle d'une activité, les entités engagent des ressources extérieures, sur une base contractuelle, qui font alors ensuite partie de l'équipe. Dans ce cas, l'objectif est de tirer parti des compétences de la ressource extérieure qui, bien que n'étant pas inscrite sur la liste de paie du service, s'imprègnera des valeurs et de la culture du service et participera pleinement à ses activités quotidiennes. Cette activité, dénommé internalisation, diffère de l'externalisation. Il est généralement estimé que les activités ou les services qui sont externalisés ne doivent pas avoir de valeur stratégique pour l'entité et que, pour attirer les compétences ayant une importance stratégique, il est préférable de recourir à l'internalisation.

7.1.2 Croissance de l'externalisation

La croissance de l'externalisation ces dernières années est due en partie à un changement généralisé de la philosophie des entreprises, découlant notamment dans une large mesure de l'avènement et de l'utilisation de la TIC, et de la nécessité de disposer d'un spécialiste de la TI qui ne fait pas nécessairement partie des principales fonctions ou des fonctions essentielles de l'entité.

Les entités se sont donc efforcées d'identifier une 'compétence de base', une combinaison unique d'expérience et de connaissances relatives aux activités principales de l'entité. Tous les aspects opérationnels de l'entité sont organisés autour des fonctions de base, et toute activité ou fonction qui n'est pas nécessaire pour appuyer les activités principales est alors externalisée.

Aujourd'hui, l'externalisation est non seulement utilisée par les entreprises, mais elle commence également à être utilisée par les pouvoirs publics.

Les fonctions d'une entité peuvent être externalisées dans leur intégralité ou de manière sélective. L'externalisation totale peut entraîner le démantèlement de divisions ou de services entiers et le transfert à un vendeur extérieur de l'ensemble des responsabilités liées à un produit, un service ou une fonction. L'externalisation sélective peut par ailleurs être axée sur une tâche ou une fonction unique, pour laquelle il existe des compétences plus

efficaces en dehors de l'entité qui peuvent être gérées plus efficacement par un spécialiste extérieur.

La décision d'externaliser est de nature stratégique car elle a une incidence sur la conception de l'organisation administrative et correspond au choix essentiel, sur le plan de l'organisation administrative, des fonctions pour lesquelles des connaissances sont développées et alimentées en interne, et celles pour lesquelles ces connaissances sont achetées. Les raisons de l'externalisation peuvent non seulement comprendre la diminution des coûts, mais également la réorientation des ressources vers des domaines qui intéressent l'entité au premier chef et qui sont alignés sur les compétences actuelles et de base. Pour les fonctions non essentielles, il est judicieux d'un point de vue commercial d'utiliser les ressources humaines les plus expérimentées disponibles en dehors de l'entité, par souci d'efficacité et de rentabilité.

Il est estimé que l'avantage réel réside dans la possibilité de réaffecter les ressources aux fonctions les plus importantes de la douane, éventuellement en accordant davantage d'importance aux compétences de base des fonctionnaires des douanes.

7.2 Externalisation au sein de la douane et domaines pouvant être externalisés : activités essentielles et activités non essentielles

Le rôle de la douane dans les échanges internationaux n'a cessé d'évoluer. Le commerce mondial repose de plus en plus sur la circulation rapide des biens et des services aux frontières. La facilitation des échanges est considérée comme un élément important de la politique économique d'un pays.

L'utilisation des progrès de la TIC permet de réorganiser les procédures avec souplesse. Les entreprises attendent de meilleurs services et souhaitent pouvoir travailler depuis leurs locaux.

La douane joue un rôle essentiel dans la chaîne logistique internationale. L'on attend de la douane qu'elle réduise le coût des transactions et de la gestion des inventaires à flux tendu, en vue de garantir la compétitivité. La douane doit donc répondre à ces attentes en offrant à temps ses services.

Ces dernières années, l'importance accrue accordée à la sécurité et à la sécurisation des échanges a obligé la douane à redéfinir sa manière de travailler. Elle doit donc élaborer une méthode permettant non seulement de satisfaire les besoins divergents de la lutte contre la fraude et de la facilitation de manière plus rentable, mais également d'offrir de manière simple aux entreprises internationales des services de qualité et d'assurer la circulation ininterrompue des biens et des services aux frontières. Le rôle de la douane s'est donc élargi et comprend celui d'un prestataire de services.

L'on n'attend pas de la douane qu'elle externalise ses fonctions essentielles dans le domaine de la sécurité, du respect des prohibitions et des restrictions, de la protection de la société ou du recueil des recettes; pour les mécanismes de livraison, l'externalisation peut être le complément des capacités internes. La plupart des services offerts appellent l'utilisation de la TIC, ce qui nécessite des compétences professionnelles en matière de TIC

qui ne relèvent pas de la compétence de la douane. En fait, l'externalisation en tant qu'option devient nécessaire lorsque la qualité du service est de la plus haute importance. Dans ce contexte, l'externalisation garantit non seulement l'efficacité, mais constitue également une valeur ajoutée pour les entreprises. Les activités douanières qui peuvent être externalisées, en permettant à la douane de se concentrer sur ses fonctions essentielles, sont notamment les suivantes :

i) gestion et fonctionnement de l'infrastructure de la douane en matière de TI;
ii) diffusion de l'information;
iii) tenue à jour du site Web;
iv) gestion des installations;
v) gestion et tenue à jour des applications;
vi) service d'assistance et services d'aide;
vii) publicité et relations publiques;
viii) sécurité de la TI et audit dans les domaines de l'évaluation de la sécurité, de la politique en matière de sécurité et des services gérés et suivis, sécurité des locaux.

7.3 Avantages de l'externalisation

7.3.1 Retour aux activités essentielles

En externalisant les fonctions non essentielles auprès d'une entité extérieure, la douane peut se concentrer sur les domaines relevant de ses principales compétences et s'acquitter de sa mission en matière de gestion de la lutte contre la fraude et de facilitation.

L'externalisation permet de faire appel à des connaissances et à une expertise que le service ne possède pas, et contribue directement à la qualité et à l'efficacité des services qu'attendent les milieux commerciaux internationaux.

7.3.2 Responsabilité

L'externalisation repose sur le principe, partagé par l'entreprise et par le vendeur, selon lequel ces accords appellent un service de qualité en échange d'un paiement. Cette responsabilité, définie dans le cadre d'accords sur le niveau de service, est pratique et légale, et a une incidence financière. Il n'en va pas de même lorsque le service est assuré par des ressources internes.

7.3.3 Qualité

En n'engageant pas de ressources internes pour des tâches pour lesquelles il n'existe pas de ressources au sein de l'entité, on évite le problème des comportements peu efficaces et des mauvais résultats.

7.4 Enjeux de l'externalisation

7.4.1 Questions liées à la qualité des services

Dans toute situation où des tâches ou des activités sont externalisées, il existe toujours le risque d'un mauvais contrôle de qualité. Cela est particulièrement vrai si une activité doit être réalisée par la douane et par le vendeur, les responsabilités étant donc partagées. L'externalisation fonctionne mieux lorsqu'une activité complète est externalisée et que la responsabilité n'incombe donc qu'à une seule entité. Plus important encore, la

souplesse du vendeur à s'adapter rapidement à la modification de la législation et des procédures, suite à une décision d'ordre politique, affecte la livraison du service et le coût du service. L'enjeu consiste à déterminer le type de relations en matière d'externalisation qui répondra le mieux aux besoins et à le définir dans les accords sur le niveau de service.

Un autre aspect important de l'externalisation, souvent négligé, est que la responsabilité globale du service presté par le vendeur incombe à la douane. Il n'y a pas cession de la responsabilité pour la simple raison que la tâche a été confiée à une autre entité. Le vendeur preste le service aux clients au nom de la douane et une étroite implication entre la douane et le vendeur est indispensable aux fins du respect des normes de prestation de services. Il convient donc d'évaluer régulièrement la manière dont le vendeur s'acquitte de ses tâches.

7.4.2 Questions liées aux ressources humaines

Certains arguments s'opposent à l'externalisation du point de vue des ressources humaines. L'on craint en effet que l'externalisation entraîne une perte de connaissances au sein de l'entité et de loyauté de la part du personnel. A moins que le service externalisé ne soit un bien – régulièrement disponible ou un service facile à remplacer – il est préférable de le faire au sein de l'entité.

Si les ressources humaines sont indispensables au succès de l'entité, il faut investir dans ces ressources. Il vaut mieux encourir des dépenses pour former à nouveau le personnel que de réaliser des économies en réduisant les frais d'externalisation. Des ressources humaines formées et informées assureront la pérennité de la connaissance des opérations au sein de l'entité.

Les possibilités d'internalisation peuvent également être examinées lorsque les connaissances nécessaires sont temporairement indisponibles.

L'externalisation et l'internalisation présentent également un enjeu du point de vue de la délocalisation de l'emploi hors des frontières nationales.

Toutefois, l'externalisation peut également permettre de réduire la charge de travail des employés, notamment lorsque la douane est confrontée à une multiplication de ses responsabilités, mais sans bénéficier d'un accroissement de ses ressources humaines. En libérant les fonctionnaires des douanes de tâches fastidieuses, de nouvelles opportunités de formation professionnelle s'ouvrent.

7.4.3 Questions liées à la sécurité

L'externalisation des services crée des flux d'informations et de connaissances en dehors de l'entité. Des préoccupations sécuritaires naissent lorsque les données ou les informations sensibles de clients sont transmises sans autorisation, en portant atteinte à la législation nationale. Le caractère confidentiel et la protection des données ne sont pas nécessairement des infractions aussi graves à l'étranger. Le vol de données peut nuire au client sur le plan financier et imposer à l'entité qui externalise des responsabilités inacceptables sur le plan légal pouvant aller jusqu'à la fraude. Limiter l'accès aux sources d'informations mises à la disposition du vendeur constitue un problème technique. Des compromis peuvent nuire à l'entité d'une manière inacceptable.

Il convient de limiter l'accès aux informations au personnel autorisé, en fonction de ses responsabilités. Des mécanismes de contrôle approprié doivent être conçus avec soin pour accorder un accès selon les besoins ; le principe du refus de l'accès à toutes les informations, sauf si cela est absolument nécessaire aux tâches du personnel du vendeur, doit par exemple être appliqué de manière stricte. L'accès aux informations doit également être contrôlé et vérifié périodiquement.

7.5 Conclusion : comment établir l'équilibre approprié

Face à la multiplication constante des responsabilités, des contraintes en matière de coûts et de ressources humaines, de la nécessité de disposer de compétences techniques spécialisées pour offrir des services de qualité, et des opportunités qu'offrent les progrès de la technologie de l'information, l'externalisation est la voie de l'avenir.

Pour que l'externalisation soit efficace, il convient de définir les besoins du service et d'identifier un vendeur capable d'intégrer efficacement toutes les fonctions externalisées de manière à ne pas devoir chercher des vendeurs individuels pour chaque fonction.

L'externalisation ne doit pas être considérée comme la simple délégation d'une tâche à une entité extérieure, mais comme une relation de partenariat mutuellement avantageuse, dans laquelle la douane et le vendeur s'impliquent quotidiennement pour offrir des services en fonction de normes déterminées au préalable et de manière durable.

Le contrat d'externalisation doit définir clairement les responsabilités et les critères de performance, les règles de confidentialité et les droits de propriété des nouvelles idées ou techniques. Les accords concernant le niveau de service constituent un moyen concret d'évaluer les résultats obtenus en matière de performance. Le contrat doit également comporter un moyen de mettre fin aux relations si le service presté ne répond pas aux attentes.

8. INTERFACES ENTRE APPLICATIONS DE TI

La douane doit concevoir ses systèmes informatiques selon une architecture informatique intégrée pouvant comprendre les sous-systèmes d'application et les bases de données ci-après. Quand interfaces sont développées au sein des sous-systèmes exploités par les administrations douanières, elle conduit à une intégration plus étroite entre les différentes fonctions de l'organisation. Afin de construire un environnement de guichet unique pour le commerce, il peut être nécessaire de construire des interfaces avec les systèmes appartenant à d'autres organismes gouvernementaux concernés par les contrôles réglementaires transfrontalières. Interfaces de systèmes peuvent également être développés pour soutenir l'échange d'informations avec d'autres administrations des douanes (par exemple sous douanes en réseau international.)

Ce qui suit est une liste des sous-systèmes d'un système automatisé dans une administration des douanes.

Sous-systèmes d'application

- Système de traitement des déclarations à l'importation
- Système de traitement des déclarations à l'exportation
- Système de traitement des déclarations de marchandises en transit
- Système de traitement des déclarations établies aux fins des accises
- Système utilisé pour le mouvement et le contrôle des accises
- Drawback
- Gestion des risques
- Lutte contre la fraude.

Ces systèmes informatiques viennent appuyer les principaux régimes douaniers applicables aux marchandises. A cet égard, il convient d'installer entre les systèmes informatiques concernés les interfaces de communication nécessaires. Par exemple, des interfaces doivent être créées entre les systèmes traitant respectivement des opérations de transit, d'exportation et d'importation.

Bases de données de l'administration

- Enregistrement des opérateurs commerciaux
- Cette base de données peut contenir les données partenaire commercial, les garanties constituées, à quelle fin, de quel montant maximum et par quelle banque - et les dispositions spéciales prises par la douane, procédures simplifiées par exemple
- Base de données tarifaire intégrée (nomenclature)
- Y compris les mesures prises à l'échelon national et international
- Comptabilité des recettes
- Sélection
- Déclarations
- Paiements différés

L'architecture informatique devrait permettre à tous les utilisateurs concernés au sein de la douane de consulter les renseignements enregistrés. Chaque base de données peut être exploitée par plusieurs sous-systèmes d'application.

En ce qui concerne la gestion des bases de données, il est recommandé d'enregistrer les renseignements connexes dans une seule et même base de données. Ces renseignements ainsi que les données nécessaires pour les gérer doivent donc dans la mesure du possible être enregistrés dans la même base de données. Les rapports existant entre les renseignements et leur organisation doivent être déterminés lors de l'analyse initiale du système.

Il est recommandé au moment de la conception des systèmes informatiques d'établir une distinction entre l'aspect logistique des procédures douanières (traitement) et les renseignements utiles à l'application douanière (fichiers, bases de données). Cette manière de procéder facilite la réutilisation des composants fonctionnels du système et rend plus efficace la tenue à jour des systèmes informatiques. L'appendice 4 contient un diagramme illustrant les relations entre certaines procédures importantes et les bases de données correspondantes.

Dans un environnement de guichet unique, les interfaces servent souvent à relier les systèmes douaniers à ceux exploités par d'autres organismes gouvernementaux. (Veuillez vous référer au Recueil de l'OMD sur la façon de construire un environnement de guichet unique). Des interfaces électroniques peuvent également être intégrées afin de communiquer avec les autres administrations douanières. Pour une description initiale des DRI, veuillez consulter la section 9.3.

8.1 Architecture orientée services

La facilité avec laquelle différentes applications sont élaborées et intégrées dépend de la manière dont elles ont été construites et assemblées. Chaque application ou module contribue à dispenser un ensemble de services visant à assurer les fonctions essentielles de contrôle des importation, des exportations et du transit mais aussi à faciliter les échanges.

L'architecture orientée services (ou SOA pour Service-Oriented Architecture) met avant tout l'accent sur les services aux entreprises. Elle ne met pas en avant l'infrastructure technique (serveurs, stockage, etc.) ni les services techniques connexes. La SOA est une approche d'architecture technologiquement neutre. Cette approche est solidement ancrée dans les services aux entreprises et constitue dès lors un choix raisonnable pour concevoir l'architecture de solutions de TI où doivent être intégrés différents éléments d'application.

L'architecture orientée services peut faciliter la mise en oeuvre de changements dans des systèmes d'information, et lier différents modules ou fonctionnalités. Les systèmes informatiques traditionnels ont été constitués en intégrant de façon rigide du matériel, des logiciels et des réseaux, rendant le tout difficile à mettre en oeuvre. L'architecture orientée services conseille le développement d'applications logicielles en utilisant des composants faciles à assembler et développer. Ces éléments constitutifs ne sont pas des logiciels, mais des services aux entreprises qui sont prestés pour répondre à des besoins précis d'entreprises. Des services fréquemment utilisés euvent être réassemblés afin de créer de nouveaux services. L'OASIS (Organization for the Advancement of Structured Information

Standards) a développé un modèle de référence standard pour l'architecture orientée services (Comité technique de l"OASIS sur la SOA, 2006).

Le concept de composants de service réutilisables est extrêmement utile. Malgré des différences dans les domaines de la réglementation, la plupart des organismes de réglementation des flux transfrontières nécessitent des services opérationnels communs. Ceux-ci ont trait à l'inspection de fret, de personnel d'équipage et de moyens de transport, à l'examen documentaire, à l'enregistrement de résultats de tests, au prélèvement d'échantillons, au calcul de droits et taxes, au cadre d'évaluation des risques, etc. Ces composants de service sont réutilisables non seulement pour des opérations commerciales, mais également pour les logiciels sous-jacents. Si l'objet des inspections peut varier entre des organismes gouvernementaux, les étapes du processus sont les mêmes, et si les paramètres de calcul de droits, taxes et redevances peuvent varier, tous sont liés au processus de perception et de prélèvement. Les services de paiement peuvent servir à tous les paiements qui surviennent au cours du dédouanement du fret.

Les composants de la technologie de l'information (TI) sur lesquels s'appuient les services réutilisables sont des éléments constitutifs qui peuvent s'associer de manière souple. C'est précisément ce qui permet la réutilisation de composants. Ces possibilités de combinaison flexible ou couplage lâche réduisent l'impact de changements. L'architecture orientée services repose sur une terminologie courante où l'usager du service (qui se trouve être un composant logiciel) nécessite un service d'un fournisseur de services (un autre composant logiciel). L'échange de demande de service et de prestation de service repose sur des messages et la qualité du service est régie par des contrats de service entre les composants de service en interaction.

Ces caractéristiques exigent qu'un « service » soit une unité autonome dont les performances ne dépendent pas de l'état d'autres services. Il s'agit de l'incarnation logique de fonctionnalités autonomes. Ce caractère autonome d'un composant de service permet aux développeurs de logiciels de l'enlever, d'apporter des changements et de le replacer sans que cela n'ait d'impact sur d'autres composants. Les services peuvent être orchestrés. Cela implique que des services puissent être réagencés ou réorganisés pour s'adapter à l'objectif commercial. Il s'agit d'un atout considérable dans le traitement de processus opérationnels au sein d'un environnement de guichet unique. Le schéma ci-dessous illustre la capacité de composants SOA d'être orchestrés comme suit:

Evaluation des risques/ Service d'évaluation des risques/ Examen des marchandises/ Service d'examen matériel/ Examen des documents/ Service d'examen des documents/ Orchestration n° 1

Evaluation des risques/ Service d'évaluation des risques/ Examen des documents/ Service d'examen des documents/ Examen des marchandises/ Service d'examen matériel/ Orchestration n° 2

La communication entre les différents services passe par des messages. Pour veiller à la bonne collaboration entre les services, ces messages doivent être interopérables et être compatibles avec les différentes plates-formes. Ces messages doivent être capables de décrire et découvrir des services. Le tout doit être fiable et sécurisé, en se fondant sur des normes de l'industrie.

L'une des façons d'assurer l'interface entre les différentes applications existantes consiste à les modifier pour qu'elles fassent partie d'une Architecture orientée services (SOA). Ce processus s'appelle la "préparation à la SOA". Il est recommandé d'y recourir afin d'assurer l'intégration entre les applications.

9. ECHANGE DE RENSEIGNEMENTS

(Normes 3.11 et 7.2)

9.1 Echanges de renseignements avec les opérateurs commerciaux

Le concept d'échange de renseignements entre la douane et les opérateurs commerciaux a évolué, pour finalement déboucher sur une approche de « Guichet unique ». Cette notion de Guichet unique s'est récemment imposée pour le commerce international et les échanges réglementaires transfrontières. Le guichet unique procède à l'analyse des contrôles officiels du point de vue de l'opérateur commercial et envisage toutes les interactions possibles entre les opérateurs commerciaux et les organismes de réglementation en faisant abstraction des départements au sein de l'administration. Une telle approche met indéniablement en lumière toutes les redondances dans les procédures, les doublons dans les formalités et globalement le manque de rentabilité au moment de remplir les formalités liées à la réglementation transfrontière. Cette approche analytique permet d'identifier une série de solutions pour simplifier considérablement l'interface entre l'administration et les opérateurs commerciaux en donnant une nouvelle orientation aux procédures et en réorganisant les données nécessaires pour la réglementation.

Il existe différents types d'interactions entre la douane et les opérateurs commerciaux, cependant les principaux échanges de renseignements entre la douane et les opérateurs commerciaux concernent l'importation et l'exportation de marchandises.

Il existe plusieurs normes permettant de présenter les renseignements électroniques sous la forme de fichiers informatiques. Il s'agit de normes de syntaxe. La norme de syntaxe la plus couramment employée est la norme EDIFACT/ONU, constitué par les répertoires des Nations Unies pour l'Echange de données informatisé pour l'administration, le commerce et le transport. L'utilisation du langage XML (langage de balisage extensible) a progressé avec le développement des technologies Internet. Il existe des normes régionales ainsi que des normes propres à un secteur d'activité, telles que "ANSI X.12" et "CargoIMP". Les syntaxes propriétaires non standardisées de messages sont aussi couramment répandues. Les syntaxes propriétaires sont considérées comme coûteuses puisque leur compréhension et leur utilisation imposent aux professionnels d'allouer des ressources nouvelles.

Depuis bien longtemps, la douane effectue aux frontières des contrôles lors desquels elle exige et utilise des éléments de fait sur le transport, la manutention du fret, la localisation des chaînes logistiques, les marchandises, le conditionnement, l'inspection, l'évaluation, les droits et taxes etc. Malgré de remarquables évolutions technologiques et en dépit des innovations qu'ont connues les régimes douaniers et les procédures opérationnelles, la douane continue plus ou moins à traiter les mêmes renseignements opérationnels de base. Ces fragments d'information ont été méthodiquement incorporés aux Modèle de données de l'OMD.

Le Modèle de données de l'OMD est un ensemble d'exigences de données soigneusement combinées qui se renforcent mutuellement et seront mises à jour de manière régulière pour répondre aux besoins sur le plan juridique et des procédures des agences aux frontières chargées de la réglementation des flux transfrontières telles que les douanes, pour le contrôle des transactions d'exportation, d'importation et de transit. Cet instrument est élaboré et tenu à jour par l'Equipe de projet chargée du Modèle de données et sa promotion est assurée par le biais de partenariats avec des Membres de l'OMD, des organisations internationales et le secteur privé.

Le Modèle de données de l'OMD se présente sous la forme d'une bibliothèque contenant deux parties principales : la première partie se présente sous la forme d'un recueil de composantes normalisées et la seconde partie regroupe les Dossiers d'information. Les Dossiers d'information sont construits à partir de composantes du modèle de données et représentent l'utilisation des données dans les procédures opérationnelles. Ils fournissent des modèles électroniques pour l'échange de renseignements. Ils peuvent également servir à illustrer des fonctions opérationnelles. L'Appendice 1, intitulé " Structures de l'information et des télécommunications pour le commerce électronique ", offre une description détaillée des Dossiers d'information.

9.2 Echanges de renseignements avec d'autres administrations

(Norme 7.4)

De nombreux renseignements sont échangés entre la douane et les autres Organismes de réglementation des flux transfrontières, par exemple, les statistiques commerciales et les renseignements relatifs aux contingents quantitatifs, aux restrictions, aux accords préférentiels, etc. Lorsqu'il est impossible de regrouper les administrations, les délais nécessaires pour échanger les renseignements peuvent être réduits en installant une interface informatique entre les services concernés.

Lorsque les entreprises peuvent présenter par voie électronique les licences d'importation/d'exportation, les certificats sanitaires/phytosanitaires, etc. délivrés par d'autres administrations, l'interface informatique permet de confirmer instantanément à la douane la validité de ces documents.

Par ailleurs, on peut contribuer à accélérer le dédouanement de tous les envois en établissant une procédure permettant aux entreprises de communiquer en une fois à un "guichet unique" tous les renseignements à caractère réglementaire requis. Toutefois, pour garantir le bon fonctionnement d'une telle procédure, les entreprises doivent obtenir les renseignements concernant les exigences réglementaires, et ce par voie électronique. Lorsqu'elle entreprend de concevoir son système informatique, la douane doit prendre en considération non seulement les interfaces avec les opérateurs commerciaux mais également celles avec les autres administrations.

A cet égard, les normes internationales en matière d'échanges de renseignements facilitent grandement la conception d'interfaces douane/partenaires commerciaux et douane /administrations publiques. L'utilisation par tous les opérateurs commerciaux de normes identiques permettra de réduire considérablement les coûts afférents aux échanges électroniques de données.

Soucieuse de contribuer au renforcement des capacités, l'OMD a élaboré un Recueil intitulé « Comment construire un environnement de Guichet unique ». Ce Recueil contient deux volumes. Le Volume 1, intitulé « Guide exécutif », traite des aspects du Guichet unique qui concernent les cadres dirigeants. Le Volume 2, appelé « Le guide pratique » est un recueil d'outils et de techniques destinés à soutenir les experts techniques qui travaillent sur des projets de mise en place d'un Guichet unique.

9.3 Echanges de renseignements avec d'autres administrations des douanes

(Norme 7.4)

La Technologies de l'information et de la communication offre à une administration des douanes la capacité d'échanger des données avec d'autres administrations des douanes.

L'initiative de l'OMD sur les Douanes en réseau international (DRI) vise à procéder à une analyse exhaustive des possibilités de rationaliser, d'harmoniser et de normaliser l'échange sûr et efficace d'informations entre les administrations des douanes. L'analyse a permis de conclure que la manière la plus efficace de tirer parti des avantages optimaux de la coopération douane-douane serait de rationaliser les processus d'échange d'informations, ce dont pourraient également bénéficier d'autres parties prenantes.

Il s'agit d'une méthode normalisée, qui utilise des modèles et des plans génériques, facilite et améliore ces processus en accélérant la rédaction et la mise en œuvre des accords d'échange d'informations. L'élaboration d'un catalogue d'arrangements documentés de manière normalisée, dont chacun peut être reproduit avec un minimum d'effort, permet en outre d'accélérer l'extension, le développement et l'accès aux réseaux douaniers.

Au plan bilatéral, multilatéral et plurilatéral, les administrations des douanes continuent d'œuvrer à des arrangements et à des accords qui permettent pleinement de partager des informations de la manière la plus efficace possible. L'échange d'informations s'effectue suivant deux axes : l'un concerne les informations liées à la lutte contre la fraude et l'autre porte sur les informations relatives aux flux commerciaux de marchandises.

Il existe déjà un Réseau douanier de lutte contre la fraude, qui contribue à une diffusion rapide d'informations sensibles, non nominatives, dans le domaine de la lutte contre la fraude. On recense de nombreux exemples d'échanges d'informations entre les administrations douanières, en vigueur aux niveaux bilatéral et régional. L'initiative des Douanes en réseau international s'appuie sur le concept de « Bloc utilitaire » pour décrire l'échange d'informations entre les douanes.

Un bloc utilitaire est une partie spécifique du processus opérationnel de la douane, expliquée en termes simples mais complets, compréhensibles par tous. Un bloc utilitaire décrit les objectifs stratégiques pour les décideurs, les processus opérationnels pour le personnel d'encadrement, les questions juridiques pour les juristes, les méthodes fonctionnelles pour les fonctionnaires chargés des opérations et les spécifications techniques pour le personnel chargé de la TI. Il est construit et examiné par des experts au moyen d'un modèle de conception normalisé. Il est axé sur les besoins d'une partie précise du processus

opérationnel de la douane, y compris les éléments de données pertinents, par exemple opérateurs économiques agréés (OEA), fraude commerciale, transit, etc.

La décomposition des processus opérationnels de la douane en blocs utilitaires individuels permet aux autorités douanières d'être sélectives quant aux processus opérationnels et aux informations connexes qu'elles choisissent de partager avec leurs partenaires, et de conclure plus rapidement ces arrangements de mise en réseau.

Le partage de renseignements préalables, la reconnaissance mutuelle des Opérateurs économiques agréés (OEA), la reconnaissance mutuelle des contrôles, la coordination des contrôles sur le transit et le partage transfrontières d'une déclaration d'exportation de marchandises d'un pays en vue de son utilisation dans le pays importateur sont quelques-uns des exemples de « Blocs utilitaires » en cours d'élaboration.

L'emploi à des fins douanières de la RUE de l'OMD pourrait aider grandement l'échange de renseignements à l'échelon international (voir l'appendice 9). Ainsi que l'indique son nom, ce numéro de référence serait utilisé pendant toute la durée de la transaction et constituerait un moyen d'identification unique de la transaction par tous les intervenants. La douane devrait envisager de prévoir un tel champ de données lorsqu'elle conçoit ses bases de données concernant les transactions.

Les échanges de renseignements à l'échelon international peuvent soulever des questions en matière de droit et de procédure qui devront être examinées. Les administrations qui s'engagent dans cette voie devraient faire appel, dès le lancement du projet, à des juristes nationaux compétents pour s'assurer que les modifications éventuellement nécessaires sur le plan législatif sont apportées en temps voulu.

10. COMMUNICATIONS

(Norme 7.2)

Les administrations des douanes qui s'engagent dans la voie de l'EDI doivent être conscientes que le succès de leur entreprise dépendra de la disponibilité et de la facilité d'accès du système. La seule garantie dans ce domaine consiste à utiliser à tous les échelons de la conception du système des normes reconnues à l'échelon international. Les normes internationales revêtent un intérêt particulier dans quatre domaines.

10.1 Solutions en matière de transmission des données

Il existe trois possibilités dans ce domaine :

1. la livraison matérielle sur un support magnétique tel que bandes et disquettes, par voie postale ou par l'intermédiaire de services de courrier;
2. la transmission « de point à point »; et
3. les réseaux de communication qui offrent des services de stockage, d'envoi, et d'autres services à valeur ajoutée.

Bande/disquette

Cette méthode est lente; elle exige en effet que le support soit expédié par la voie postale ou que l'opérateur commercial se rende dans les locaux de la douane. Elle peut être considérée comme un premier pas dans la voie du commerce électronique. Comme indiqué dans le Modèle de données douanières de l'OMD, des messages normalisés internationaux peuvent être utilisés. Enfin, la mise en oeuvre de ce système permettra à la douane et aux entreprises d'acquérir une expérience pratique précieuse en matière de commerce électronique.

Point à Point

Un modem permet à deux ordinateurs de communiquer par l'intermédiaire des lignes téléphoniques ou par liaison satellite. Toutefois, les lignes téléphoniques traditionnelles sont destinées aux communications vocales et non pas informatiques, il faut donc disposer de modems et de logiciels de télécommunication pour pouvoir échanger des renseignements par ce biais.

Lorsque des lignes numériques spécialisées sont utilisées en lieu et place des lignes téléphoniques commutées normales, les systèmes informatiques expéditeurs et destinataires peuvent utiliser un contrôleur de transmission plutôt qu'un modem. La principale différence entre les lignes commutées et les lignes spécialisées se situe au niveau de la vitesse. La vitesse de transmission sur les lignes commutées est nettement inférieure, de sorte qu'elles ne sont adaptées qu'à la transmission de faibles volumes de données.

Réseaux de communication

Dans le cadre d'un réseau de communication type, chaque opérateur commercial souhaitant échanger des renseignements dispose d'une boite à lettres électronique, qui est

gérée par le réseau. Les messages électroniques sont transmis par l'intermédiaire du réseau, d'une boite à lettres à une autre. Il s'ensuit que contrairement à la communication point à point, qui exige que les deux systèmes soient disponibles et puissent recevoir des données en même temps, la transmission et le stockage temporaire des données sont dissociés du système d'application. Si pour une raison quelconque le système douanier ne fonctionne pas, les opérateurs commerciaux peuvent continuer à envoyer des renseignements dans la boite à lettres de la douane.

Un réseau à valeur ajoutée (VAN) est un réseau de communication appartenant à un tiers qui est capable d'accepter des messages de toute configuration informatique et de les transmettre à un destinataire qui utilise un matériel et des logiciels différents. Un VAN offre non seulement des services de communication mais également des services de traduction et de sécurité en matière d'EDI. La plupart des VAN acceptent un large éventail de protocoles de communication. Etant donné que les technologies de communication et les protocoles de conversion peuvent devenir extrêmement complexes, un VAN offre un véritable service à valeur ajoutée en se chargeant de cet aspect des communications entre deux opérateurs commerciaux, ou au sein de groupes d'opérateurs, disposant de configurations informatiques différentes.

La douane devra déterminer les moyens les plus efficaces de recevoir des renseignements. Dans de nombreux pays, il n'existe pas de service de type VAN; en revanche, Internet y est accessible. Ce réseau est généralement moins onéreux que les VAN, mais pour l'heure, Internet soulève des problèmes sur le plan de la sécurité et du niveau des services.

En dehors des réseaux à valeur ajoutée, certaines administrations se tournent déjà vers Internet comme moyen principal d'échanger des informations.

10.2 Télécommunications

S'agissant des télécommunications, la douane doit s'assurer que les protocoles utilisés pour la connexité matérielle sont reconnus (par exemple, les protocoles X21, X25, X400, etc., de l'Organisation internationale de normalisation (ISO)). Il existe également des normes pour les protocoles d'Internet, par exemple TCP/IP et HTTP. Ces normes sont généralement utilisées par les prestataires de services de télécommunications, les réseaux à valeur ajoutée et les prestataires de services Internet.

10.3 Conception des messages

(Normes 3.11 et 7.2)

La douane a pu effectivement exercer une influence plus directe sur la conception des normes informatiques. Ces dernières années, elle a participé à la mise au point de messages normalisés sous l'égide des Nations Unies. Ces messages EDIFACT/ONU constituent désormais une norme internationale en matière d'EDI. L'OMD a élaboré le Modèle de données de l'OMD, qui a permis d'optimiser l'échange de données par voie électronique. Ce modèle constitue un langage universel pour l'échange de données transfrontières et représente une norme mondiale de données exigées au passage des frontières pour la mainlevée et le dédouanement des marchandises, des conteneurs, des moyens de transport et des personnes ;

Les messages EDIFACT/ONU et autres messages EDI peuvent être transmis par Internet en tant que pièces jointes à du courrier électronique normal au moyen du Protocole SMTP. Ces messages électroniques peuvent être sécurisés par une signature numérique en utilisant le Protocole S/MIME.

Le développement et la généralisation rapide d'Internet offrent aux échanges de renseignements de nouvelles perspectives. En conséquence, de nouveaux formats d'échange de renseignements deviendront de facto des normes internationales parce qu'ils sont utilisés à l'échelon mondial; par exemple les formulaires électroniques, le langage hypertexte HTML, le langage "eXtensible Markup Language – XML", un répertoire mondial, l'architecture de documents ouverte (ODA), etc. Nombre de ces formats sont toujours en cours d'élaboration mais les administrations des douanes qui s'intéressent aux échanges de données informatisés futurs devront les prendre en considération lorsqu'elles définiront leur stratégie en la matière.

Internet offre aux petites et moyennes entreprises la possibilité de connaître la situation de leurs marchandises et/ou celle de leurs déclarations de marchandises vis-à-vis de la douane et leur permettra à l'avenir d'effectuer des paiements électroniques et d'archiver des documents électroniques.

L'échange de données électronique (EDI) consiste en un ensemble de protocoles d'échange de données par voie électronique permettant d'assurer des échanges structurés entre les organisations. Les normes d'origine établissent la méthode de conditionnement dans une enveloppe MIME des jeux de transactions EDIFACT/ONU. Toutefois, avec la croissance de l'Internet et la demande de services neutres et interopérables, de nouvelles normes appelées EDIINT (EDI – Internet Intégration) ont été élaborées et portent sur des questions de sécurité telle que la confidentialité, l'authenticité, l'intégrité et la non-répudiation des messages. L'Internet Engineering Task Force a géré l'évolution de ces normes, qui sont apparues à l'origine sous la forme de Demandes d'observations (Request for Comment ou RFC) contenant des "Déclarations d'applicabilité".

AS1 – Déclaration d'applicabilité décrivant comment les messages EDI sont transmis avec les normes Internet MIME et SMTP. La transmission des messages est sécurisée par le biais de signatures numériques et par le chiffrement des renseignements échangés. Le protocole AS1 permet des échanges sécurisés sur Internet.

AS2 – Déclaration d'applicabilité décrivant comment les messages EDI peuvent être transmis en temps réel à travers un échange de renseignements sur la base du protocole http et de la norme MIME. Cette méthode repose sur la signature numérique des données échangées, mais la session comme les fichiers des données échangées sont chiffrés. Le protocole AS2 assure un échange sécurisé en temps réel entre des applications basées sur le Web.

AS3 – Déclaration d'applicabilité décrivant comment les données EDI ou XML peuvent être transmises sur Internet de manière sécurisée grâce un protocole FTP de transfert de fichiers. La sécurité est assurée par le chiffrement de la session FTP, ainsi que le chiffrement et la signature des fichiers de données échangés.

Récemment, une nouvelle norme AS4 est apparue et s'appuie sur des services Web qui fournissent la technique centrale de transport des messages, tout en garantissant que les

impératifs de sécurité exigés aux fins du transport des messages sur Internet sont respectés au même titre qu'avec les protocoles AS2 et AS3.

11. SECURITE EN MATIERE DE TIC

Les activités réalisées par les gouvernements et les entreprises ont considérablement évolué au cours de ces dix dernières années. L'utilisation d'Internet et l'accès généralisé à une TIC peu onéreuse permettent aux systèmes de communiquer avec des personnes d'horizons divers qui savent de mieux en mieux comment employer et manipuler la TIC.

Ces changements ont apporté de nombreux avantages en termes de rapidité et d'accès, mais ils ont également entraîné une prise de conscience accrue des risques sécuritaires auxquels sont exposés nos communications, nos systèmes et nos banques d'information.

Le développement de la fraude informatique et les risques de sabotage et de panne accidentelle des systèmes sont quelques-uns des enjeux auxquels les administrations des douanes utilisant la TIC doivent faire face pour gérer leurs systèmes et les procédures y relatives. La corruption des systèmes de TIC douaniers ou l'intrusion dans ces systèmes peuvent entraver gravement les échanges et le recouvrement des recettes. Dans les cas les plus graves, elles risquent même de porter atteinte à la sécurité nationale.

Il est particulièrement important que les administrations des douanes définissent les risques et conçoivent une approche intégrée qui couvre non seulement les points faibles sur le plan matériel et technique, mais également la question de la gouvernance (à savoir, procédures et dispositions prises avec les entreprises) nécessaire pour assurer un degré élevé de sécurité en matière de TIC.

Les experts plaident en faveur d'une approche de gestion des risques pour gérer les risques afférents à la sécurité informatique. Les administrations des douanes devraient disposer des renseignements et des outils qui contribuent à gérer et à identifier efficacement les risques liés à leurs actifs des technologies de l'information et de la communication (TIC). L'évaluation des risques consiste à définir les menaces qui pèsent sur ces actifs ainsi que leurs failles mais aussi à estimer la probabilité et les conséquences d'un manquement aux règles de sécurité. Afin de garantir une bonne gestion de la sécurité de l'information, les compétences en matière d'évaluation des risques sont essentielles. Les risques qui pèsent sur les actifs de TI sont les incendies, les inondations, la perte d'accès, les attaques du cyberespace, les violations d'accès, la perte de données, etc. Une approche de gestion des risques aide à définir ces risques et prépare l'organisation à réduire ces risques et à répondre de manière appropriée.

La Norme ISO 27001 porte sur le Système de gestion de la sécurité de l'information, dont elle fixe les exigences. Cette norme prévoit la réalisation d'une évaluation spécifique des risques avant de sélectionner et d'appliquer une mesure de contrôle. Une démarche reposant sur la gestion des risques est décrite dans la norme ISO/IEC 27005:2011, Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information. Chaque contrôle doit être justifié par une évaluation des risques. Lorsqu'elle porte sur chaque actif de TIC concerné, l'évaluation des risques permet de budgétiser des contre-mesures proportionnées aux pertes ou aux dommages qui pourraient résulter d'une violation des règles de sécurité concernant ces actifs. Ce principe de gestion

de la sécurité de la TI doit être incorporé à la politique de sécurité évoquée dans la section 11.2 ci-dessous.

La gravité des risques liés à la sécurité des actifs de la TIC requiert toute l'attention des dirigeants de la douane car ces risques concernent des données importantes bénéficiant d'une protection juridique, des informations sur des transactions ayant des conséquences financières et des menaces sur la santé et la sécurité publiques d'un pays. La douane ne peut se permettre de perdre ces données ou de les voir exposées. Au vu des conséquences d'une violation ou d'une perte des informations (par exemple, la perte de la confiance du public), la gestion stratégique des risques liés à la sécurité de l'information doit être confiée à la direction exécutive.

11.1 Sécurité en matière de TIC – Définition et objectif

La norme ISO 27000:2012 , (Technologie de l'information - code de pratique pour la gestion de la sécurité de l'information) – définit la sécurité de l'information comme suit :

"…préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information"

la confidentialité consistant à "n'assurer l'accès à l'information qu'aux personnes autorisées"; l'intégrité à "sauvegarder l'exactitude et le caractère complet de l'information et des méthodes de traitement"; et la disponibilité à veiller à ce que seuls "les utilisateurs autorisés aient accès à l'information et aux éléments associés".

11.2 Politique en matière de sécurité de la TIC

L'un des moyens d'atteindre cet objectif est de publier une politique en matière de sécurité de la TIC, de manière à s'assurer que tous les membres du personnel connaissent les questions qui se posent, ainsi que leurs responsabilités personnelles en la matière.

Cette politique doit prouver que les cadres supérieurs ont arrêté une approche et se sont engagés à l'égard de la sécurité de la TIC et énoncer ce que l'administration attend de son personnel. Le rôle, les responsabilités et les obligations des usagers doivent également être définis de manière générale.

Bien qu'il soit possible d'informer simplement les clients de la politique arrêtée en matière de TIC, il est parfois plus approprié d'élaborer avec les usagers des accords qui énoncent clairement quelles sont les obligations et les responsabilités des clients.

Toutefois, ce n'est pas la politique en matière de sécurité de la TIC en soi qui apportera "confiance, éthique et disponibilité". Dans toute installation conçue pour la TIC, un jeu complexe de procédures, de solutions techniques, d'obligations légales et de grands principes, de procédures de gestion et de considérations pratiques sera indispensable pour sous-tendre la politique générale de l'administration en matière de sécurité de la TIC.

11.3 Sécurité de la TIC – Aspects à prendre en compte

Remarque: Pour une sécurité plus rigoureux de traitement des TIC s'il vous plaît se référer à la norme (Code de pratique pour l'information contrôles ou CoP sécurité: ISO / IEC FDIS 27002:2013).

La sécurité de la TIC couvre tous les aspects ci-après des activités d'une administration douanière :

- organisation de la sécurité de l'information
- sécurité des ressources humaines
- gestion des avoirs
-
- contrôle de l'accès
- cryptographie
- sécurité matérielle et environnementale
- sécurité des opérations
- sécurité des communications et des opérations
- acquisition, conception et tenue à jour des systèmes,
- relations avec les fournisseurs
- gestion des incidents liés à la sécurité de l'information
- aspects de la gestion de la continuité des activités liés à la sécurité de l'information
- respect de la loi.

Ces aspects sont couverts en détail dans la norme ISO 27002:2013 et il est recommandé aux administrations des douanes d'étudier de manière approfondie les considérations et les explications qui y figurent.

Les rubriques ci-après, extraites de la norme ISO 27002:2013 , contribuent à définir les grands domaines à prendre en considération dans le cadre de la sécurité de la TIC.

Organisation de la sécurité de l'information

Il s'agit du cadre de gestion permettant de mettre en place et de contrôler les dispositifs de sécurité au sein de l'administration. Il doit couvrir les rôles, les responsabilités et la séparation des tâches.

Elle comprend la création d'une infrastructure interne de gestion visant à attribuer et à maintenir les responsabilités et les rôles en matière de sécurité, et la possibilité d'exercer certains contrôles aux fins des contacts avec les autorités, des contacts avec des groupes d'intérêts spéciaux et de la sécurité de l'information dans le cadre de la gestion des projets Elle couvre également les prestataires de services, par exemple, la prestation externalisée de services de TIC.

L'utilisation de dispositifs mobiles et le recours au télétravail doivent figurer dans cette partie.

Sécurité des ressources humaines

Les dispositions liées au respect de la sécurité et la formation du personnel sont importantes pour garantir un niveau approprié de confiance et des pratiques saines. Il peut en outre s'avérer utile d'envisager de conclure des accords en matière de confidentialité et d'arrêter des modalités et des conditions d'emploi spécifiques, selon la nature des informations et de l'accès au système dont disposent les employés.

Le respect des règles de sécurité doit être évalué dans le cadre de procédures permettant de contrôler et de signaler les atteintes portées à la sécurité.

Cela comprend des contrôles spécifiques en matière de sélection, les modalités et conditions d'emploi en cours d'emploi, la gestion des responsabilités et la sensibilisation, l'apprentissage et la formation.

Gestion des avoirs

Pour protéger les avoirs en matière de TIC, notamment les banques d'informations, l'administration doit disposer d'une part d'un moyen de comptabiliser les avoirs et les informations et d'autre part d'un moyen de les classer en vue de prévoir les niveaux de protection appropriés.

Les avoirs peuvent comprendre tant l'infrastructure matérielle que les bases de données, les fichiers et les applications de logiciels qui font le cas échéant partie des avoirs matériels. Pour chaque avoir, il convient de déterminer le propriétaire, l'utilisation acceptable et la restitution. Un inventaire des avoirs doit être établi.

Les informations doivent être classées non seulement aux fins de leur traitement sécuritaire, mais également en ce qui concerne le niveau de sécurité à prévoir. Ce dernier détermine la protection dont l'information doit bénéficier (par exemple, par qui et dans quelles circonstances elle peut être consultée) et peut même déterminer la nature des avoirs matériels (matériel, installations, etc.) dans lesquels elle peut être stockée ou par lesquels elle peut être transmise. Les informations doivent être étiquetées.

Les supports qui contiennent des informations doivent être gérés de manière appropriée. Il convient de décrire la gestion, la cession et le transfert matériel des supports amovibles.

Contrôle de l'accès

Le contrôle de l'accès à l'information est la clé de la création de systèmes sécurisés en lesquels les usagers ont confiance.

L'accès doit reposer sur les prescriptions fixées par l'administration pour s'assurer que seules les autorités appropriées pourront consulter ou transmettre certaines informations. Ces prescriptions sont généralement énoncées en détail dans une "politique de contrôle d'accès" qui fixe les modalités et les critères permettant de déterminer l'accès aux systèmes et à l'information.

Outre la manière dont les contrôles d'accès doivent être gérés, les services concernés devront déterminer :

- qui est chargé d'accorder l'accès
- les règles régissant l'octroi de l'accès
- les niveaux et les types d'accès à prévoir, et
- les privilèges liés aux différents niveaux et types d'accès.

Il s'avère parfois nécessaire d'élaborer des règles de gestion de l'accès pour résoudre des questions comme, par exemple, le temps qui peut s'écouler avant qu'une session inactive soit automatiquement fermée, les conditions préalables à l'accès à certaines zones du système et même la modification des autorisations qui peut être automatique ou soumise à la décision des cadres supérieurs.

Les contrôles d'accès au réseau et la surveillance des accès sont également importants car les connexions au réseau peuvent représenter un risque significatif en matière de sécurité. Les aspects importants de l'accès au réseau comprennent notamment les moyens par lesquels :

- les utilisateurs sont authentifiés
- les terminaux et autres points d'entrée sont identifiés et consignés, et
- les chemins empruntés par les utilisateurs sont contrôlés.

La question de l'authentification des utilisateurs et des possibilités les plus fréquemment retenues en la matière est traitée en détail dans la partie 10.4 - Authentification.

Les responsabilités de l'utilisateur et le contrôle de l'accès à l'application et au système doivent également figurer dans cette partie.***Cryptographie***

La cryptographie doit être utilisée de manière appropriée et efficace pour protéger la confidentialité, l'authenticité, l'intégrité et la non-repudiation de l'information.

L'emploi de la cryptographie doit être décrit dans une politique, de même que la gestion des clés cryptographiques.

Sécurité matérielle et environnementale

Lors de la conception d'une politique en matière de sécurité de la TIC et de sécurité matérielle, il est indispensable de prévoir tout risque matériel potentiel auquel pourraient être exposés les locaux abritant la TIC, le matériel de la TIC lui-même ou l'environnement de travail de la TIC.

Les contre-mesures peuvent aller de la création d'un périmètre de sécurité à des points de contrôle de la sécurité, au principe du bureau et de l'écran vides, à une alimentation électrique de secours, un câblage sécurisé, des procédures et des mesures de sécurité pour le matériel installé à l'extérieur. La sélection et l'emploi de toute contre-mesure dépendent des risques spécifiques, des différents équipements installés et de l'environnement matériel.

Sécurité des opérations

Pour s'assurer que les facilités de traitement de l'administration douanière sont convenablement sécurisées, il convient de fixer des procédures adéquates.

Cet aspect couvre diverses questions, notamment :

- documentation et application de procédures d'exploitation
- gestion du changement
- mesures nécessaires pour séparer différents environnements de TIC tels que mise à l'essai et production
- planification à long terme de la capacité, de l'acceptation des nouveaux systèmes ou des mises à niveau
- protection contre des logiciels hostiles
- gestion interne
- sauvegardes
- enregistrement et surveillance.

Sécurité des communications

- contrôles et gestion du réseau
- ségrégation dans les réseaux
- transfert d'informations et accords relatifs aux transferts d'informations
- messagerie électronique.
-

Des précisions complémentaires concernant les échanges d'informations et de logiciels figurent dans la partie 10.4 – Authentification qui couvre nombre des facteurs que les services doivent analyser pour garantir l'intégrité de l'information et déterminer l'identité des parties qui communiquent.

Acquisition, conception et tenue à jour des systèmes

La sécurité doit faire partie intégrante de la conception des systèmes et comprendre l'infrastructure, les applications et les procédures de soutien.

Lors du remplacement, de la sélection ou de l'acceptation de logiciels, il convient de prendre des précautions afin d'éviter les voies clandestines ("porte dérobée" qui permet un accès non autorisé) et les chevaux de Troie. Le contrôle de l'accès aux fins des changements de codes, le recours à des fournisseurs de confiance, la vérification des codes et la mise à l'essai des produits constituent quelques-unes des stratégies possibles. Il convient de veiller à protéger de manière appropriée les données destinées aux mises à l'essai.

Relations avec les fournisseurs

Les relations avec les fournisseurs doivent envisager les aspects suivants :

- politique de sécurité liée aux relations avec les fournisseurs
- question de la sécurité prévue dans les accords
- chaîne logistique de la technologie

- surveillance et examen des services des fournisseurs
- gestion des changements dans les services des fournisseurs

Gestion des incidents liés à la sécurité de l'information

Il est indispensable de gérer les incidents liés à la sécurité. Il convient de décrire les responsabilités et les procédures en la matière. Les événements et les points faibles doivent être notifiés aussi rapidement que possible au personnel d'encadrement. Lorsque survient un événement lié à la sécurité de l'information, il convient de l'évaluer, d'y faire face et de recueillir des éléments de preuve à son sujet.

Les enseignements tirés de chaque événement doivent réduire la probabilité ou l'incidence des futurs événements.***Aspects de la gestion de la continuité des activités liés à la sécurité de l'information***Les conséquences d'une défaillance, suite à une défaillance de la sécurité ou à un sinistre, doivent être prises en considération avant d'élaborer et de mettre à l'essai un plan de continuité des activités.

Comme dans tout aspect de la planification de la sécurité, les mesures de continuité des activités adoptées dépendront des risques définis, de la probabilité que ces risques se concrétisent et des conséquences pour les activités de l'administration. Pour de nombreuses administrations des douanes, une défaillance dans la prestation des services peut non seulement interrompre les échanges, mais également nuire à la sécurité nationale en affaiblissant les fonctions de ciblage, de sélection, d'établissement de profils et de communication.

Pour garantir la disponibilité des facilités de traitement de l'information, celles-ci doivent être mises en oeuvre avec suffisamment de redondance.

Respect de la loi

Il convient de tenir compte des mesures permettant de s'assurer que l'administration respecte les exigences juridiques ou contractuelles auxquelles elle est soumise, ainsi que ses cadres et principes internes de sécurité.

Les aspects à prendre ne compte sont notamment les droits d'auteur, la protection des dossiers administratifs, la gestion des dossiers recevables comme éléments de preuve et le contrôle des listes de vérification.

11.4 Authentification

11.4.1 Pourquoi l'authentification est-elle nécessaire ?

Dans un environnement sur papier, les procédures et conventions concernant l'authentification de l'identité et des documents ont été approuvés il y a longtemps. A titre d'exemple, des moyens tels que signatures écrites, signatures de témoins et sceaux sont utilisés pour authentifier l'identité. Le développement de moyens légaux et judiciaires visant à "prouver" l'authenticité de l'identité d'une partie et de ses liens avec ses transactions a pris beaucoup de temps et, même s'ils ne sont pas infaillibles, ces moyens ont fait leurs preuves dans le cadre des systèmes judiciaires de différents pays.

Il n'est pas toujours possible de transférer ces méthodes dans un environnement électronique et les nouvelles méthodes d'authentification doivent encore être évaluées et adoptées.

L'enjeu de l'authentification est encore plus important dans un environnement électronique en raison :

- de l'ampleur de l'accès offert par la TIC
- du volume croissant des transactions, et
- de la 'distance' par rapport au client (sur le plan géographique et en termes de relations) qui est encouragée par les transactions électroniques.

Cet aspect revêt une importance particulière pour les administrations des douanes s'agissant de leur rôle en matière de respect de la loi et de lutte contre la fraude. Tout échec dans l'établissement d'un lien solide entre un particulier et son identité, ses documents ou ses déclarations électroniques nuirait à la qualité des éléments de preuve présentés devant la justice. Il pourrait en outre exposer les systèmes de la douane à un risque de fraude ou d'utilisation abusive de l'identité, sapant ainsi la confiance des usagers dans les systèmes et la réputation d'une administration.

11.4.2 Variantes électroniques

Diverses possibilités s'offrent en matière d'authentification ; elles varient considérablement en fonction du degré d'assurance de l'identité offert et du degré de fiabilité avec lequel une partie peut être liée à son message.

Les méthodes d'authentification vont d'un simple système de mot de passe aux systèmes complexes qu'offre la cryptographie à clé publique. Chaque méthode ou technique présente ses propres points forts et ses propres points faibles. Les diverses méthodes disponibles sont brièvement décrites ci-dessous.

Mots de passe, NIP et ID de l'utilisateur

Pour les systèmes informatiques, la méthode d'authentification la plus fréquente est aujourd'hui le mot de passe. Bien que plusieurs techniques et méthodes d'authentification différentes soient actuellement utilisées, authentification à base de jetons, reposant sur la biométrie ou sur les connaissances par exemple, les méthodes d'authentification par noms d'utilisateur et mots de passe comportant un texte (alphanumérique) continuent d'être utilisées. Cette partie traite donc des meilleures pratiques concernant la qualité des mots de passe.

Le mot de passe repose sur le principe qu'il n'est connu que de son détenteur et de son émetteur, l'accès n'étant possible que lorsque le mot de passe de l'utilisateur correspond aux fichiers de la partie émettrice. Comme de nombreux systèmes d'authentification, il oblige l'utilisateur à préserver la sécurité de son identité en ligne – son mot de passe.

Du point de vue technique, le modèle du mot de passe peut faire l'objet d'attaques "par force brute", par exemple "par dictionnaire". Ces attaques consistent généralement en tentatives informatiques répétées visant à obtenir un accès non autorisé par tâtonnements. Pour cette raison, les systèmes de mots de passe reposent sur la sécurité des voies par

lesquelles le mot de passe est communiqué et sur les pratiques et les dispositions prises en matière de sécurité par la partie émettrice.

Au mieux, un mot de passe authentifie l'identité de l'utilisateur ; il ne permet pas d'authentifier les documents communiqués, ni de vérifier l'intégrité de la teneur du message.

Les systèmes de mots de passe présentent certes l'avantage d'être mis en place à peu de frais, mais ils sont mieux adaptés à une utilisation unique ou dans des cas où les données ou le système à protéger présentent un faible niveau de sécurité.

Les systèmes de mots de passe peuvent être sécurisés davantage en les associant à d'autres méthodes de sécurité et d'authentification telles que le cryptage, les ID d'utilisateurs ou le système de l'interrogation par le dispositif répondeur.

Il est indispensable d'appliquer une bonne pratique de gestion des mots de passe. Les décisions de politique générale du personnel d'encadrement détermineront l'efficacité de tout système de mot de passe et le niveau de soutien nécessaire à la tenue à jour des usagers. Ces décisions peuvent comprendre des principes simples en matière de sécurité concernant des questions telles que :

- la longueur, la composition et la durée de vie des mots de passe
- le nombre d'échecs d'ouverture de session autorisé
- les procédures et processus permettant d'émettre, de ré-émettre et d'annuler les mots de passe, etc
- veiller à ce que les utilisateurs demeurent conscients de la nécessité de protéger convenablement leur mot de passe.

Mots de passe à utilisation unique

Les mots de passe à utilisation unique surmontent le principal inconvénient des systèmes conventionnels de mots de passe, à savoir, le fait que le mot de passe peut être perdu, volé ou parfois violé, puis utilisé de manière répétée sans autorisation.

Le système de mot de passe à utilisation unique crée un mot de passe unique pour chaque session, et ce généralement grâce à une unité de matériel connectée qui génère automatiquement un mot de passe. Le système de l'administration douanière sait quels sont les mots de passe ou les séquences associés à tel ou tel utilisateur et n'autorise l'accès que s'il y a correspondance entre les deux.

Cette méthode présente l'inconvénient d'obliger tous les utilisateurs à acheter, ou à être équipés, du matériel et du logiciel nécessaires. Une mise en oeuvre sur une base large peut s'avérer onéreuse et être mieux adaptée à un groupe d'utilisateurs hétérogènes. Un point faible que partage ce système avec d'autres systèmes d'authentification est qu'il dépend lui aussi des pratiques sécuritaires appliquées par les utilisateurs pour contrôler leur dispositif de mot de passe et le moyen d'y accéder.

Système de l'interrogation par le dispositif répondeur

Ce système est fréquemment utilisé en association avec d'autres méthodes comme les mots de passe.

Le principe est le suivant : l'utilisateur fournit des réponses à une question à laquelle il est le seul à pouvoir répondre. Dans certaines versions, l'utilisateur peut même être invité à suggérer la question. Les questions servent ensuite à "tester" l'identité de la personne lorsque, par exemple, les dossiers de l'utilisateur doivent être modifiés ou qu'un nouveau mot de passe doit être délivré. Ce système peut également être utilisé comme moyen de vérification complémentaire de l'authentification lors de l'ouverture de la session.

Selon l'approche et les besoins de l'administration, le système de l'interrogation par le dispositif répondeur peut s'avérer d'un fonctionnement compliqué. Le processus de gestion du système peut entraîner des dépenses importantes et avoir une incidence financière continue pour l'administration.

Témoins («Cookies»)

Les «témoins» sont des marques apparaissant dans l'ordinateur d'un utilisateur qui peuvent servir à reconnaître la machine d'un utilisateur.

Pour authentifier un utilisateur, les témoins partent du principe que chaque machine n'est utilisée que par une seule entité. Ils ne sauraient donc être considérés comme un moyen fiable d'authentifier une identité précise.

Dans la mesure où les témoins peuvent servir à suivre les habitudes de navigation d'un individu, leur utilisation abusive soulève parfois de graves questions de confidentialité. Les témoins peuvent également être volés et utilisés pour accéder frauduleusement aux systèmes d'une administration. En outre, leur niveau d'acceptation par les utilisateurs est relativement faible.

Biométrie

La plupart des méthodes d'authentification n'associent pas l'identité matérielle à l'utilisateur lorsque ce dernier accède aux systèmes de l'administration. La biométrie vise à résoudre cette question en établissant un lien direct entre les caractéristiques physiologiques ou comportementales connues d'un individu et celles de l'utilisateur.

Les caractéristiques de la voix, les empreintes digitales ou la paume de la main, la rétine ou le visage, qui sont uniques, sont codés numériquement et comparés par un dispositif de reconnaissance chaque fois que l'utilisateur souhaite accéder au système.

La biométrie repose sur le fait que l'utilisateur doit disposer de matériel de reconnaissance chaque fois qu'il doit accéder aux systèmes de l'administration. Elle repose aussi sur la sécurité du code numérique qui représente l'identité de l'intéressé.

Outre qu'elle est onéreuse, l'application large de la biométrie risque de rencontrer des difficultés s'agissant de l'acceptation par les utilisateurs de certaines des méthodes de reconnaissance employées – par exemple, dans de nombreuses cultures, la reconnaissance de l'iris est considérée comme une atteinte à la vie privée.

Chiffrement conventionnel

Le chiffrement conventionnel est plus connu sous le nom de "cryptographie symétrique". S'agissant des algorithmes symétriques, l'émetteur et le récepteur doivent

utiliser le même code (un fichier informatique assorti d'un code d'identification unique également dénommé code secret). Prenons un exemple très simple : si le message à transmettre est le chiffre 20, l'émetteur et le récepteur peuvent convenir que l'algorithme qu'ils utiliseront consistera à soustraire ce code du message. Les deux parties pourraient alors convenir que le code sera le chiffre 2. L'émetteur codifie le message en "18", le transmet, et le récepteur le décrypte en ajoutant le code permettant d'obtenir à nouveau le chiffre 20. Tant qu'un algorithme complexe est utilisé et que les deux parties conservent leur code en lieu sûr, la confidentialité est pratiquement garantie. Le traitement des algorithmes symétriques est généralement plus rapide.

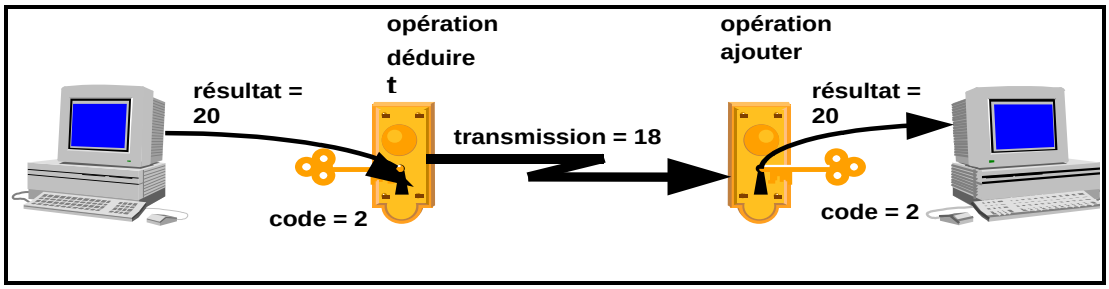


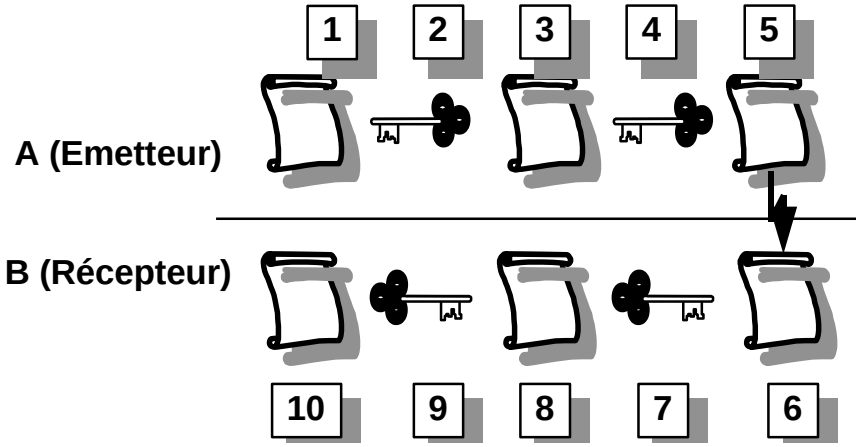
Schéma 2: Eléments d'un système utilisant des codes symétriques

Le principal point faible du système réside toutefois dans l'émission et la distribution des codes qui permettent à l'utilisateur et à l'émetteur de s'identifier l'un l'autre. Non seulement un jeu de codes distinct doit être convenu avec chaque utilisateur, mais les codes doivent en outre être matériellement fournis au client en vue de préserver un certain degré de certitude quant à l'identité. Lorsque des services de messageries ou des tiers acheminent les codes, la sécurité de l'identité risque d'être compromise. Le traitement des algorithmes symétriques est certes rapide en matière de chiffrement et de déchiffrement, mais la gestion de base nécessaire pour garantir l'authentification peut s'avérer onéreuse et peu commode si le système est utilisé sur une base large.

Cryptographie à code public (certificats numériques)

Les problèmes de la distribution des codes liés au chiffrement conventionnel sont résolus par la cryptographie à code public. La cryptographie à code public utilise en effet des paires de codes distincts aux fins de l'authentification (ou signature) et du chiffrement (ou confidentialité). Ces paires de codes sont dénommées codes publics et codes privés. La cryptographie à code public est souvent qualifiée d'‘asymétrique' puisque les codes publics et privés sont différents.

Le code privé n'est connu que de son propriétaire alors que le code public peut être publié et connu de tous. Un message chiffré au moyen du code public du récepteur ne peut être déchiffré qu'en utilisant le code privé correspondant. Dans le cadre de la norme RSA (du nom de ses inventeurs), les codes sont construits à partir de manipulations de deux nombres premiers très grands, mais les notions mathématiques qui régissent les algorithmes sont trop complexes pour être expliquées ici. Chacun peut donc crypter un message destiné à un récepteur donné, dans la mesure où il connaît son code public. L'inconvénient d'utiliser des codes asymétriques est que les calculs prennent beaucoup plus de temps.



1. Document en clair sans signature électronique
2. Code privé de A servant à crypter la valeur de contrôle des données + horodateur (= signature numérique) (intégrité)
3. Document en clair avec signature électronique
4. Algorithme symétrique servant à crypter la teneur (confidentialité)
5. Document crypté avec signature électronique
6. Document égal à 5
7. Algorithme symétrique servant à décrypter la teneur (contrôle de la confidentialité)
8. Document égal à 3
9. Calcul de la valeur de contrôle des données + horodateur; code public de A servant
10. à décrypter la valeur de contrôle reçue; rapprochement des deux valeurs (contrôle de l'intégrité) Document égal à 1

Schéma 3 : Organisation d'un système de cryptage reposant sur des codes publics

La cryptographie asymétrique résout certains problèmes éventuellement liés à la distribution des codes, mais elle oblige toujours l'utilisateur à assurer la sécurité de ses codes. Elle soulève également des questions concernant la manière dont l'identité de l'utilisateur est validée lors de l'émission du code.

Infrastructure à clé publique

L'Infrastructure à clé publique (ICP) vise à résoudre les problèmes que ne parvient pas à résoudre la cryptographie asymétrique conventionnelle. L'ICP utilise la cryptographie asymétrique comme base technique et offre un cadre permettant de sécuriser la teneur des messages, d'authentifier l'émetteur et de valider son identité.

Ces objectifs sont atteints en introduisant un certificat numérique, c'est-à-dire un document électronique signé par une autorité de certification de confiance qui identifie le propriétaire de la clé et l'entité commerciale (le cas échéant) qu'il représente. Elle lie le propriétaire de la clé à une paire de clés en précisant quelle est la clé publique de cette paire de clés.

L'ICP comporte un jeu complexe d'éléments juridiques et administratifs qui lui permettent de fonctionner efficacement. Ces éléments, associés au fonctionnement de l'ICP, sont traités plus en détail dans la partie 10.9.

L'ICP présente des points forts, dans le cadre d'une seule et même solution, dans le domaine de l'authentification, de l'intégrité des messages, de la confidentialité et de la non-répudiation.

L'un de ses points faibles est toutefois qu'elle s'appuie sur les procédés utilisés par des tiers pour vérifier les identités et délivrer des certificats compte tenu de ces vérifications. Il est possible d'y remédier en élaborant des spécifications plus strictes ou en réalisant cette fonction au sein de l'administration, mais moyennant un coût supplémentaire.

Les pratiques de gestion et de sécurité appliquées par le détenteur du certificat constituent un autre point faible. Si le détenteur perd (ou permet à d'autres d'utiliser) son certificat, il devient impossible de se fier à son authentification.

Transport Layer Security (TLS)

Le protocole Secure Sockets Layer (SSL) est un jeu de règles régissant l'authentification des serveurs (serveurs Web par exemple) et les communications cryptées entre les clients et les serveurs. Ce protocole a été conçu pour sécuriser la transmission des données sur Internet. Le processus d'authentification sous SSL utilise le chiffrement des clés publiques et les signatures numériques pour confirmer qu'un serveur est bien le serveur qu'il prétend être. Il n'authentifie pas l'utilisateur. Une fois que le serveur a été authentifié, le client et le serveur utilisent des techniques de chiffrement à clés symétriques pour chiffrer les informations qu'ils échangent. Une clé de session différente est utilisée pour chaque transaction afin d'empêcher tout pirate informatique de déchiffrer les messagesLe protocole Transport Layer Security (TLS) a ensuite été conçu en tant qu'extension du SSL, Version 3.0.

Il convient de souligner que le protocole SSL et le protocole Transport Layer Security (TLS) assurent uniquement la confidentialité et l'intégrité du serveur. Ils n'assurent pas la non-répudiation et, à moins d'être appuyés par une protection appropriée des clés privées, associée à la volonté et à la capacité de l'utilisateur à valider les certificats numériques, ils n'offrent pas une authentification efficace. Le SSL est bien connu du fait de son utilisation dans les navigateurs Netscape et Internet Explorer sur le Web.

En mai 1996, la responsabilité du développement du SSL a été confiée à une organisation internationale de normalisation, l'Internet Engineering Task Force (IETF), qui conçoit de nombreuses normes de protocoles pour Internet. Le TLS, version améliorée du SSL, a été lancé début 1999 et étendu en tant que TLS 1.2. Le protocole Transport Layer Security est une technologie très largement utilisée et certaines versions de ce produit peuvent être utilisées par les administrations des douanes.

11.4.3 Quelle méthode utiliser ?

"Quelle est la solution à retenir en matière d'authentification ?" est une question importante à laquelle il n'existe pas de réponse unique correcte. L'approche adoptée doit être déterminée par le résultat de l'évaluation des risques et compte tenu de l'élaboration d'un argumentaire y relatif. Le choix de toute méthode ou combinaison de méthodes dépendra des risques et des conséquences auxquelles une administration serait confrontée si une identité s'avérait fausse ou si des transactions et des informations étaient répudiées. Il dépendra également du coût relatif et de l'environnement dans lequel travaille l'administration concernée.

11.4.4 Risques acceptables

Plusieurs procédés bien conçus permettent déjà de définir, d'évaluer et de gérer les risques. L'un des premiers a été la norme AS/NZS4360.1999 (www.standards.com.au) de l'Australie et de la Nouvelle-Zélande. Cette norme figure également dans la norme ISO/IEC 27005:2011, Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information, dont la section 3.14 concernant l'évaluation des risques définit cette dernière comme un processus de comparaison entre les résultats de l'analyse des risques et les critères de risque en vue de déterminer si le risque et/ou son ampleur est acceptable ou tolérable [SOURCE: ISO Guide 73:2009]. Il peut exister d'autres normes nationales et il est recommandé aux administrations d'envisager de consulter ces documents lorsqu'elles évaluent les risques.

Pour définir et évaluer les risques en situation, l'administration concernée doit étudier:

- l'environnement dans lequel elle travaille – notamment les facteurs de nature politique, économique, technique, commercial et juridique qui affectent ses opérations
- ses clients et les relations qu'elle entretient avec eux
- la nature des transactions effectuées et
- ses besoins et ses opérations.

L'administration obtiendra ainsi une vue d'ensemble des domaines qui présentent pour elle des risques. Par exemple, le contexte politique peut obliger l'administration à fournir aux usagers un large accès à des transactions en ligne. L'administration devra donc traiter avec différents groupes de clients, dont certains avec lesquels elle a conclu depuis longtemps des accords en matière de respect de la loi et d'autres qui n'effectueront peut-être qu'une seule transaction. L'environnement juridique d'une administration publique peut obliger cette dernière à utiliser ses propres transactions comme éléments de preuve en cas de poursuites judiciaires, d'où la nécessité de prévoir la non-répudiation des transactions. Les dangers et les points faibles constatés compte tenu de ces considérations constituent les risques que l'administration doit effectivement évaluer.

L'évaluation des risques consiste généralement à étudier les répercussions de chaque risque et les probabilités qu'il a de se concrétiser – plus les conséquences sont graves et plus la probabilité qu'il se concrétise est grande, et moins ce risque sera acceptable. Les risques peuvent ensuite être assortis d'un ordre de priorité, les contre-mesures existantes évaluées et de nouvelles définies si nécessaire. Il est peut probable que tous les risques puissent être supprimés et, en tout état de cause, cela serait trop onéreux. L'évaluation doit reconnaître que toutes les méthodes d'authentification ne sont pas totalement fiables et sûres. Chacune d'elles peut être compromise par quiconque possède les compétences et les ressources nécessaires, ou en raison du caractère inadéquat de sa mise en oeuvre, des pratiques ou des procédures de sécurité appliquées.

La mise en place d'un système informatique très sûr, mais onéreux, peut en fait n'offrir qu'un avantage marginal par rapport à d'autres solutions en termes de dissuasion ou de diminution des risques, et ne justifie pas nécessairement les frais supplémentaires ainsi encourus.

L'objectif est de s'assurer que les risques sont ramenés à un niveau acceptable et que les mesures adoptées auront un effet dissuasif sur les menaces auquel le système est

exposé. A titre d'exemple, une administration peut avoir constaté qu'elle est exposée dans le cadre de ses transactions électroniques à un risque de répudiation dû au fait qu'elle n'est pas en mesure de s'assurer de l'identité de l'entité avec laquelle elle communique. Elle estime alors que les conséquences risquent d'être graves – fraude en matière d'identité, perte de recettes et commerce illicite. Décidant qu'elle a besoin du degré d'authentification et de sécurité le plus élevé possible, l'administration envisage une solution d'ICP, assortie d'exigences renforcées en matière de preuve de l'identité et d'un contrôle plus strict de l'annulation des certificats. Toutefois, les certificats numériques sont aujourd'hui quatre fois plus onéreux, peu de vendeurs proposent d'appuyer les besoins de l'administration, et les efforts et les frais sur le plan administratif s'en trouveront considérablement accrus.

En étudiant de manière plus approfondie les probabilités que les risques se concrétisent, l'administration constate que ses groupes de clients présentent des caractéristiques différentes et représentent différents aspects de ses activités. Elle constate qu'elle effectue la plupart de ses transactions avec des clients de confiance avec lesquels elle a conclu depuis longtemps des accords en matière de respect de la loi et applique des procédures transparentes. Pour ces clients au moins, l'administration peut faire face aux risques en adoptant une approche beaucoup moins coûteuse et perfectionnée.

11.4.5 Comparaison des méthodes d'authentification

Pour déterminer quelles sont les solutions adéquates en matière de gestion des risques, les administrations devront évaluer et comparer les méthodes d'authentification. Plusieurs de ces méthodes sont abordées dans le paragraphe 10.4.2 qui indique également leurs points forts et leurs points faibles respectifs.

Lorsque l'on compare toutes ces méthodes, il importe de se rappeler qu'il n'existe pas de solution unique et qu'il est possible d'utiliser une combinaison de méthodes pour atteindre des niveaux plus élevés d'authentification et de sécurité. Par exemple, pour effectuer de simples transactions financières de faible valeur, il est courant d'utiliser des NIP ou des mots de passe, associés à une autre forme de chiffrement. De même, le système de l'interrogation par le dispositif répondeur est souvent utilisé non pas en tant que principal moyen d'authentification, mais plutôt en tant que contrôle secondaire aux fins de la mise à jour des informations de l'utilisateur dans des transactions présentant des risques faibles à modérés.

Chaque méthode doit être évaluée compte tenu des besoins de l'administration et des risques déterminés. Une méthode appropriée peut ensuite être choisie en fonction du degré de précision avec lequel elle permet de répondre aux besoins de l'administration et de la mesure dans laquelle elle ramène à un niveau acceptable les risques auxquels l'administration est exposée. En outre, plusieurs méthodes peuvent être utilisées en parallèle, auquel cas il conviendra également de déterminer comment elles fonctionnent ensemble.

11.5 Non-répudiation

La non-répudiation est une question qui intéresse tout particulièrement les administrations des douanes qui exercent généralement des fonctions en matière de réglementation, de perception des recettes et de contrôle des frontières. Les rapports, les

déclarations et la présentation de documents sont souvent obligatoires aux termes de la loi et les pénalités en cas d'infraction à ces dispositions font souvent l'objet de poursuites judiciaires.

Les administrations des douanes doivent donc étudier sérieusement la mesure dans laquelle elles peuvent associer avec précision les transactions et la teneur des messages avec un expéditeur donné. Elles doivent également étudier comment elles peuvent s'assurer qu'une fois placées sous leur contrôle, les informations ne sont pas corrompues ou transformées de manière à ne plus constituer de preuves recevables.

11.5.1 Définition de la non-répudiation

Il existe un problème inhérent, et souvent non énoncé, à la notion de 'non-répudiation'. Au plan technique, ce terme signifie l'utilisation de méthodes de cryptographie par une partie de confiance afin d'apporter la preuve qu'un message n'a pu être expédié que par le signataire et par personne d'autre. Cela signifie généralement que des procédures techniques doivent être utilisées pour identifier le signataire, assurer l'intégrité du message et établir un lien entre le signataire et le message. Ce processus peut également être étendu de manière à couvrir l'établissement d'un lien entre le message et le destinataire. Toutefois, d'un point de vue juridique, le principe de la non-répudiation n'existe pas. Dans certains cas, quels que soient les éléments de preuve recueillis grâce à ces méthodes de cryptographie, il est toujours possible pour quelqu'un de nier l'incidence juridique d'une transaction. En effet, il est uniquement possible de limiter les risques de répudiation.

Malgré ces anomalies, la non-répudiation peut généralement être définie comme suit: "l'assurance raisonnable qu'un lien peut être clairement établi entre une entité et une transaction afin de lier cette entité aux conséquences juridiques de ladite transaction."

La non-répudiation a pour objet de fournir une certitude sur le plan technique et juridique. Alors que les exigences techniques et commerciales peuvent entraîner l'élaboration de principes de non-répudiation, il s'agit néanmoins d'une question juridique. La non-répudiation doit être considérée compte tenu de ses éventuelles conséquences futures sur le plan juridique.

11.5.2 La non-répudiation n'est pas une question isolée

La non-répudiation n'est que l'une des questions à examiner par toute administration qui souhaite élaborer un système pour les transactions ou effectuer des transactions électroniques. Les politiques et procédures en matière de non-répudiation doivent être considérées comme faisant partie de la technique de gestion des risques qui couvre plusieurs autres questions tout aussi importantes, notamment, même si la liste n'est pas exhaustive :

- la confidentialité
- le coût (pour l'administration des douanes et ses clients)
- la convivialité
- la sécurité
- les obligations juridiques applicables à l'échelon national aux services publics en général (par exemple, toute législation générale couvrant la confidentialité, la liberté d'information, la tenue de la comptabilité, etc.)

- les prescriptions juridiques s'appliquant expressément à la douane (par exemple, la législation relative à la douane et aux accises ou, dans certains cas, la sécurité nationale)

La politique et la solution juridique/technique spécialement retenues par une administration en matière de non-répudiation dépendent des besoins de cette administration dans ces différents domaines.

11.5.3 Incidence de la répudiation sur le plan juridique

Il n'existe pas de politique unique en matière de non-répudiation, ni de solution juridique, commerciale ou technique unique permettant de limiter la répudiation et applicable à toutes les administrations. Les architectures, les politiques et les procédés adoptés par les administrations pour éviter la répudiation varient en fonction de leurs besoins et de la nature des conséquences juridiques dont elles souhaitent assortir leurs transactions.

De manière générale, les conséquences juridiques des transactions relèvent de quatre catégories qui sont toutes pertinentes pour les administrations des douanes :

Infractions pénales :

Applicables aux transactions officielles ou conformes à la loi. Les administrations devront tenir compte du niveau de preuve exigé sur le plan pénal (intime conviction), des obligations à remplir pour être jugé par un jury, et des conditions particulières à réunir en matière légale pour engager des poursuites au pénal.

Poursuites civiles :

Applicables aux transactions commerciales (l'administration achète ou vend des biens ou des services). Les poursuites engagées au civil concernent généralement des contrats de droit privé, mais d'autres moyens peuvent également être appliqués ; ainsi, certains pays appliquent des dispositions législatives particulières en matière commerciale. Dans ce cas, les administrations peuvent spécifier d'autres formes de règlement des litiges telles que l'arbitrage ou la médiation.

Contentieux administratif *:*

Applicable lorsque la transaction conduit à une décision allant à l'encontre du client. Certains pays possèdent un double degré de juridiction pour ces décisions. I convient alors d'examiner des questions telles que la nécessité de garantir les principes élémentaires du droit du client.

Mesures d'exécution :

La méthode la plus efficace pour l'administration des douanes consiste parfois à refuser au client la possibilité de traiter avec lui par voie électronique à l'avenir, ce qui n'élimine pas la question de la répudiation d'une transaction donnée. Toutefois, dans certains cas, la perspective de perdre cet accès peut dissuader des clients de tenter de répudier une transaction. Le client peut ne disposer d'aucun droit de recours contre l'administration, mais lorsqu'il existe une instance de recours, un médiateur ou d'autres voies de recours judiciaire, les administrations doivent être en mesure de justifier leurs actes.

Une administration doit tenir compte du niveau de risque acceptable que présente la répudiation des transactions qu'elle gère. En évaluant ces risques, elle doit également prendre en considération l'équilibre à établir entre le coût et la réalisation efficace des objectifs fixés.

La solution varie beaucoup en fonction du type de transaction et des risques qui y sont associés. Pour des paiements financiers simples, la non-répudiation n'est peut-être pas à craindre, la preuve de la remise et l'encaissement étant les deux principaux risques. La nécessité de prévoir la non-répudiation sera plus importante en cas d'acceptation de garanties ou de déclarations auxquelles l'entité doit être expressément liée.

De même, les solutions différeront sensiblement en fonction de la technologie adoptée par l'administration concernée. Une administration qui utilise des NIP ou des mots de passe, par exemple, peut devoir entreprendre sa propre authentification au moyen de procédures internes et se baser sur un simple accord conclu avec les utilisateurs. Par ailleurs, une administration qui utilise l'ICP devra faire davantage confiance à des tiers et utilisera un jeu complexe d'accords allant au-delà de l'utilisateur.

11.5.4 Assurance

La non-répudiation est essentiellement un exercice de gestion des risques. Le niveau d'assurance dont une administration a besoin quant à l'identité, la teneur ou le procédé est le reflet du risque qu'un client répudie une transaction et des conséquences éventuelles de cette répudiation.

Pour qu'une affaire impliquant une transaction électronique aboutisse favorablement, il convient de recueillir des éléments de preuve (sous une forme recevable en justice, le cas échéant) concernant de nombreux aspects de la transaction, notamment :

- le processus permettant d'apporter la preuve de l'identification
- la manière dont l'identité de l'expéditeur d'une transaction électronique est garantie (par exemple, contrôle de l'accès, NIP, codes privés, etc.)
- le fait que l'administration ait ou non imposé des conditions d'utilisation
- les informations fournies aux clients concernant le contrôle de l'accès, éventuelle formation et autres représentations ou instructions
- la technique particulière d'authentification utilisée (un archivage ou un système patrimonial peut s'avérer nécessaire)
- la version du logiciel d'application utilisé par le client
- la manière dont le logiciel a été mis en place à ce moment précis, et
- la preuve du moment auquel la transaction a été effectuée.

11.5.5 Motifs de la répudiation

Les raisons pour lesquelles un client peut tenter de répudier une transaction peuvent être classées comme suit :

- **Raisons propres à la transaction électronique :** le client prétend que la transaction, ou une partie de la transaction, a été effectuée sans qu'il en ait eu connaissance ou sans son accord (falsification). Cela compromet généralement l'intégrité ou le caractère approprié des procédures ou de l'infrastructure technique dans le cadre desquelles la transaction a été effectuée.

- **Motifs juridiques de nature générale :** Le client admet que la transaction a été effectuée, mais prétend ne pas y être lié sur le plan juridique.

Les raisons propres à la transaction électronique peuvent comprendre des allégations selon lesquelles :

- la transaction a été falsifiée ou modifiée en transit par un tiers – suite à une attaque crypto-analytique ou à la perte ou au viol du code, du jeton du client, etc.
- la transaction a été falsifiée ou modifiée après réception par l'administration ou par un fonctionnaire indélicat ou un pirate extérieur qui a accédé au système de l'administration
- l'identité du client est fausse suite à un manquement du processus d'enregistrement/identité électronique.

Les motifs juridiques de nature générale pour lesquels un client peut tenter de répudier une transaction dépendent de la nature des conséquences juridiques dont l'administration souhaite assortir ses transactions. Des exemples sont fournis à l'Appendice A du présent chapitre.

Il convient de souligner qu'aux fins des transactions électroniques, la non-répudiation ne requiert pas que des solutions techniques. A titre d'exemple, il peut s'avérer approprié de concevoir une transaction en prévoyant des phases déconnectées afin de minimiser le risque de répudiation. Ainsi, un client pourrait être tenu d'imprimer un formulaire obtenu sur un site Web, de le remplir, et de le remettre ensuite à l'administration concernée ou de le lui transmettre par courrier ou par télécopieur.

L'un des motifs juridiques de nature générale de la répudiation est que le client ne connaît pas pleinement la teneur de la transaction à l'égard de laquelle il prétend avoir donné son accord. Dans une large mesure, la solution à cette difficulté réside dans la conception technique du système qui doit permettre au client de visualiser l'ensemble du contenu et, si nécessaire, de le dérouler avant qu'il n'appuie sur le bouton "accord" ou "envoyer".

11.6 Assurance de l'identité

11.6.1 Preuve de l'identité

La question tient essentiellement à l'authentification, mais les éléments de preuve servant à établir une identité électronique et les procédés utilisés pour vérifier ces éléments de preuve constituent la base indispensable pour établir un lien entre une entité et ses transactions. Tout manquement à ce premier niveau accroît le risque de répudiation des transactions reposant sur l'identité.

L'administration doit comparer le besoin d'identification électronique à son propre besoin d'authentifier l'identité et d'éviter la répudiation des transactions. Lorsque les conséquences de la répudiation deviennent plus graves, il convient de prévoir un niveau plus élevé de validation et de preuve.

Une autre complication survient lorsque des méthodes d'authentification impliquant des tiers (par exemple dans le cadre de l'ICP) et des accords spécifiques sont nécessaires pour

établir la responsabilité d'un tiers et garantir l'identité. Toutefois, ces questions sont résolues dans le cadre du « Gatekeeper Framework » concernant le fonctionnement des Autorités de certification.

11.6.2 Preuve de l'autorisation

La preuve de l'autorisation d'effectuer des transactions est particulièrement importante lorsque ce sont les agents ou les employés d'une entité qui effectuent les transactions. Il est facile de répudier une transaction lorsqu'il n'existe pas de lien évident entre l'identité électronique et l'autorisation d'utiliser cette identité.

Il importe à cet égard de conclure des accords de nature juridique pour établir une identité électronique. Le moment auquel ils sont conclus, les personnes qu'ils lient et la forme qu'ils prennent sont influencés par le type de transaction et par le système et les procédés particuliers choisis par l'administration concernée.

11.6.3 Le cadre

L'assurance de l'identité repose sur le fait que le client exerce un contrôle approprié sur les outils de vérification (tels que NIP ou codes privés) et sur le fait que l'accès à ces outils est limité à la personne appropriée. Il convient à cet égard d'étudier la question de la responsabilité de l'utilisation de l'identité, tant en ce qui concerne la responsabilité du propriétaire de sécuriser son identité que les dispositifs de protection offerts par les systèmes et procédures d'une administration pour protéger cette identité. Ces responsabilités sont généralement énoncées dans les accords conclus entre les parties.

Les administrations doivent également étudier deux autres aspects, à savoir, la manière dont les identités sont mémorisées (par exemple sur des jetons spécialisés tels que cartes à puces intelligentes ou directement sur des lecteurs de disques informatiques, le cas échéant) et la sensibilisation du client à la nécessité de s'assurer que les dossiers sont stockés de manière sûre.

11.7 Assurance du contenu

11.7.1 Assurance de l'intégrité

Au cours de la durée de vie d'une transaction, son contenu sera consulté, manipulé, traité et stocké. Pendant cette période, le contenu transmis par l'expéditeur doit pouvoir être identifié et reproduit comme la transmission d'origine. Si une administration n'est pas en mesure de reproduire le contenu et d'en prouver l'intégrité grâce aux procédés qu'elle a utilisés pour effectuer la transaction, ses actes pourront être contestés et le contenu sujet à répudiation.

Le lien entre l'identité électronique et le contenu d'une transaction revêt une importance primordiale. Sans lui, toute tentative de limiter la répudiation d'une transaction est vouée à l'échec. La gestion de cet aspect dépend de la solution technique adoptée par l'administration. Un certificat électronique faisant partie d'un courrier électronique avec un contenu joint peut aisément être séparé et des procédures administratives peuvent s'avérer nécessaires pour assurer la conservation de la communication originale complète. Un processus complètement informatisé pour les transactions peut exiger simplement la tenue à

jour d'un journal électronique détaillé des transmissions, des accès et des modifications autorisées.

11.7.2 Rassembler les différentes parties

Les transactions comportent souvent plusieurs décisions et communications électroniques décomposées. Il importe que toutes les composantes d'une transaction soient suivies et demeurent liées à ladite transaction. Si toutes les composantes ne peuvent être recherchées pour apporter la preuve de l'ensemble de la transaction, l'intégrité de cette dernière peut être mise en doute et elle peut être totalement ou partiellement répudiée.

Il convient d'envisager l'adoption de procédures appropriées comme la consignation et l'annotation.

11.7.3 Stockage et reproduction

Plusieurs questions se posent en matière de stockage et de reproduction des éléments de la transaction qui affectent la répudiation.

L'intégrité de la mémoire, la forme sous laquelle un document est stocké, la gestion et la mise à jour des mécanismes de chiffrement, s'ils sont utilisés, ainsi que les liens maintenus entre les données traitées ont tous une incidence sur la force des preuves qui limitent la répudiation.

11.8 Intégrité des processus

11.8.1 Cadre de gestion

La conception de tout processus comporte des éléments qui assurent la qualité et par conséquent l'intégrité dudit processus et des matériaux traités. Ces éléments correspondent aux points du processus permettant le mieux de limiter la répudiation. Ils comprennent généralement des questions de gouvernance comme la définition des responsabilités en matière de prise de décisions et les procédures d'autorisation et d'examen des accès.

Tous ces processus concernent l'intégrité de la transaction, ils sont essentiels quant aux assurances nécessaires pour éviter la répudiation et constitueront une importante source d'éléments de preuve si l'administration doit se défendre contre des accusations de négligence ou de fraude interne.

11.8.2 Architecture et règles du système

S'agissant de la fiabilité des documents, les tribunaux peuvent examiner l'intégrité et les capacités des systèmes électroniques utilisés. A cet égard, les diverses questions importantes pour limiter la répudiation comprennent les règles du système, les règles des logiciels et l'architecture.

Les systèmes électroniques fonctionnent dans un cadre de règles – décisions prédéterminées qui affectent les mesures prises à l'égard de chaque transaction. Ces règles peuvent concerner des aspects allant des modalités et de la portée des accès aux données qui sont consignées ou mémorisées, à quel moment et sous quelle forme. Ils doivent être examinés du point de vue des assurances qu'ils offrent.

11.9 Infrastructure à clé publique (ICP)

L'ICP est l'une des méthodes d'authentification les plus complexes. Comme son nom le laisse supposer, l'ICP n'est pas une «solution isolée» mais une «infrastructure» axée sur la cryptographie à clé publique qui comporte une structure organisationnelle et un cadre légal. Contrairement à de nombreuses autres solutions, l'ICP vise donc à offrir un ensemble complet de techniques et de procédés permettant d'assurer l'authentification et l'intégrité et de réduire les risques de répudiation.

Cette méthode n'est pas encore utilisée très largement mais elle apparaît à l'heure actuelle comme l'une des solutions les plus efficaces qui s'offrent aux entités ayant besoin d'un niveau élevé d'assurance. Dans la mesure où les administrations des douanes auront certainement cette exigence, il a été décidé de traiter de l'ICP séparément et de manière détaillée.

11.9.1 Données générales

Lorsqu'une administration des douanes décide d'autoriser les opérateurs commerciaux, les agents en douane, les transporteurs et d'autres services de réglementation à dédouaner leurs marchandises à l'importation et à l'exportation de manière sécurisée via Internet ou en faisant appel à des prestataires de services de réseaux à valeur ajoutée (RVA), elle doit parallèlement résoudre des questions de sécurité en matière de TI qui sont traitées précédemment dans le présent chapitre.

Internet est par nature un système ouvert. Ses points forts découlent de cette ouverture, de son faible coût et de sa facilité d'accès, de sorte qu'Internet constitue un moyen peu onéreux d'effectuer des transactions licites avec la douane. Toutefois, son caractère ouvert est également source de grand danger pour les internautes.

En effet, il peut porter atteinte à l'intégrité des sites Web et des communications par Internet et les capacités dont disposent les administrations des douanes en matière de TI pour transmettre des messages EDI sont elles-mêmes exposées à ces dangers. Lors de l'étude des stratégies permettant de limiter les risques, il convient de se référer aux normes actuellement élaborées par divers organismes. Le fait d'effectuer des transactions sur Internet soulève des risques qui relèvent de quatre grandes catégories. Il s'agit (a) du caractère privé d'un message, (b) de son authenticité, (c) de son intégrité et (d) de sa non répudiation. L'Infrastructure à clé publique (ICP), reposant sur la technologie de la cryptographie à clé publique, offre un moyen de limiter ces risques.

Les normes EDIINT ont été élaborées par le Groupe d'étude technique chargé de l'Internet (Internet Engineering Task Force - IETF) afin de résoudre des questions liées aux techniques sécurisées de communication des messages EDI sur Internet. Ces normes définissent l'ICP comme l'une des techniques de facilitation permettant de résoudre ces problèmes de sécurité.

11.9.2 Définition de l'ICP

L'infrastructure à clé publique peut être définie comme l'architecture, l'organisation, les techniques, les pratiques et les procédures qui ensemble appuient la mise en œuvre et le fonctionnement d'un système de cryptographie à clé publique reposant sur l'utilisation de certificats. Elle comprend un jeu de principes généraux, de procédés, de plates-formes de serveurs, de logiciels et de postes de travail, servant à gérer les clés et les certificats

numériques. Un système de cryptographie à clé publique fonctionne au moyen d'algorithmes de systèmes d'encryptage asymétriques.

11.9.3 Comparaison entre une signature conventionnelle et une signature numérique

L'ICP a pour fonction de traduire les conventions du monde matériel qui reposent sur la confiance afin de pouvoir les appliquer à des transactions en ligne. Les signatures ne constituent pas la substance de la transaction et n'en représentent qu'un aspect. Elles confèrent certaines caractéristiques aux objets qui composent la transaction. Plus précisément, une signature sur papier authentifie le signataire et un document signé ; le signataire laisse ainsi une marque distinctive et l'écrit du signataire devient la signature. Cette dernière devient elle-même la preuve qui établit un lien entre le signataire et le document signé. Le signataire d'un document sur papier connaît l'importance que revêt l'acte de signer et la finalité associée à la signature. En droit commun, l'acte même de signer implique que le signataire approuve dûment la teneur du document signé. Les documents signés représentent différents "états" ou les "étapes finales" d'une transaction et le fait d'avoir traversé certains états ou étapes finales.

Le support papier constitue la base des signatures conventionnelles et, par conséquent, en l'absence du papier, les caractéristiques d'une signature sur support papier doivent être intégrées dans les signatures numériques. La technologie de l'ICP permet de produire des signatures, de vérifier les signatures, d'archiver les documents/dossiers vérifiés et de fournir des éléments de preuve chaque fois que nécessaire. La mise en œuvre pratique de l'ICP doit donc tenir compte de tous ces aspects.

11.9.4 Durée de vie utile d'un certificat numérique

Dans le cadre de l'ICP, une personne peut demander un certificat numérique en produisant tout d'abord une paire de clés comprenant une clé publique et une clé privée. L'intéressé doit remplir un formulaire de demande de certificat numérique à des fins de signature et/ou d'authentification, et l'envoyer à une Autorité de certification.

L'Autorité de certification reçoit la demande de certificat numérique, vérifie que la paire de clés envoyée par le demandeur constitue une paire de clés cryptographiques valable, vérifie l'exactitude des renseignements fournis par le demandeur et émet ensuite un certificat numérique, signé par l'Autorité de certification elle-même.

La clé publique est publiée dans un répertoire qui répond généralement à la norme X.500 de l'Union internationale des télécommunications (UIT). Le demandeur conserve en sûreté la clé privée correspondante afin de l'utiliser dans le cadre d'une opération de cryptage et/ou de signature et/ou de vérification.

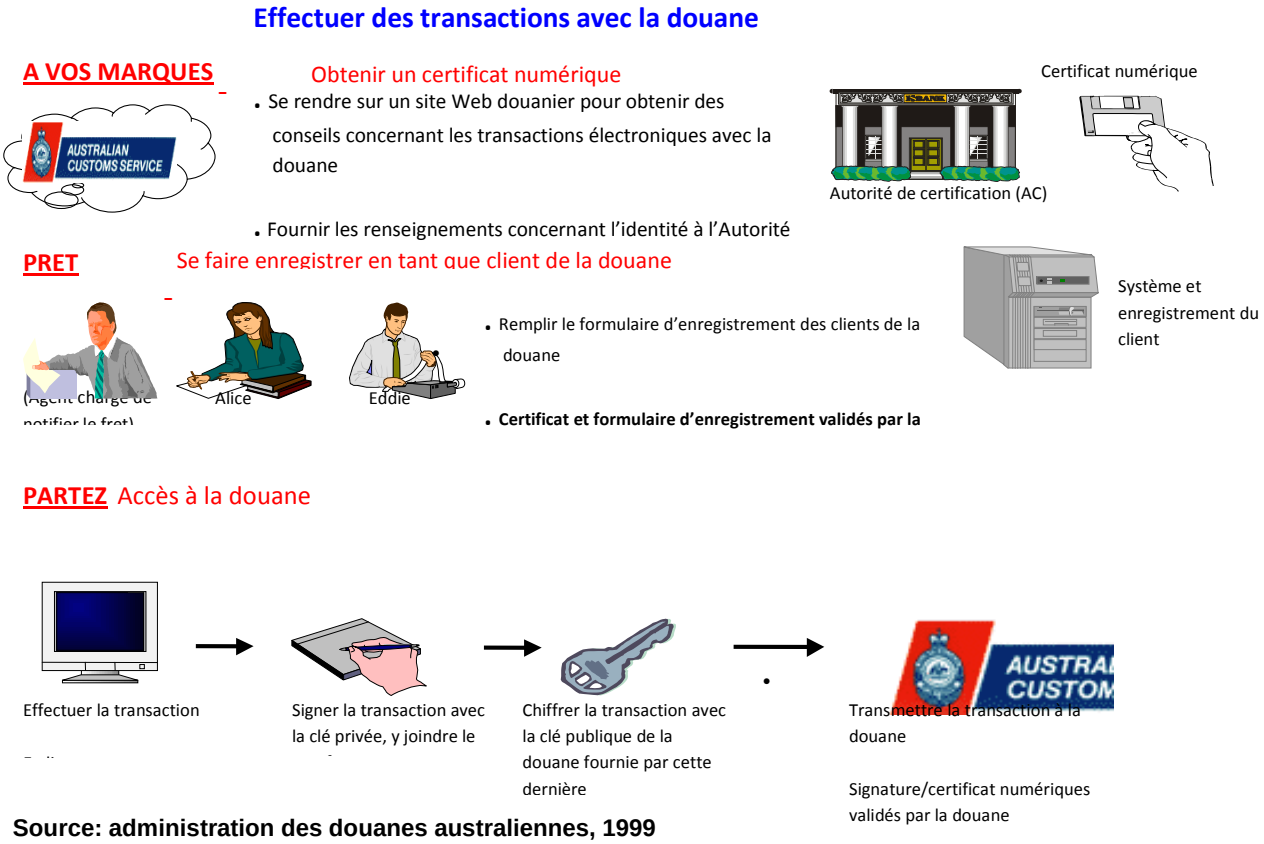
Le certificat est assorti d'un délai de validité et doit donc être périodiquement renouvelé. Pour certaines raisons précises – essentiellement, le fait de signaler une utilisation abusive ou une atteinte portée à une clé privée – l'Autorité de certification peut suspendre ou annuler le certificat numérique en cause. La durée de vie utile a été décrite dans le document RFC 2527 de l'IETF.

11.9.5 Considérations importantes liées à la mise en œuvre de solutions reposant sur l'ICP

Compte tenu des avantages qu'offre la technologie de l'ICP, les administrations des douanes pourraient envisager d'utiliser des systèmes reposant sur l'ICP lors de la conception et de la mise en œuvre de leurs solutions reposant sur les messages EDI. Il convient à cette fin de pouvoir gérer complètement les certificats et les signatures numériques dans le cadre de systèmes de TI et de procédures douanières.

La mise en œuvre de l'ICP permet de renforcer les capacités en ce qui concerne le stockage sécurisé des données électroniques et la transmission des informations électroniques au moyen des certificats (à signature) numériques. Toutefois, avant d'entreprendre la mise en oeuvre, les administrations doivent étudier la portée de leur ICP. Cette tâche consiste généralement à élaborer un « document concernant la portée du projet » qui énumère les objectifs, hypothèses et buts du projet, ainsi que les limites dont il doit être assorti.

Il importe de fixer des limites afin d'éviter que le projet ne s'étende inutilement à des domaines auxquels l'administration a déjà décidé qu'il ne s'appliquerait pas. Ce document peut comprendre des exemples de la manière dont l'administration pourra utiliser les certificats numériques à des fins d'authentification, de sécurisation des messages et de signature. Un exemple simple est fourni ci-dessous (voir figure 6). Il convient notamment de veiller à ce que la solution globale mise en œuvre par l'administration en matière d'EDI et de commerce électronique est conforme à l'ICP et compatible avec l'ICP.



Source: administration des douanes australiennes, 1999

Figure 6 : "Alice et Eddie"

11.9.6 Utilisation des signatures numériques dans les messages EDI et XML

Le Consortium du World Wide Web (W3C) et l'IETF élaborent actuellement une signature numérique normalisée pour les messages XML. Le CEFACT/ONU et l'OASIS s'efforcent d'intégrer le Protocole SOAP (Simple Object Access Protocol) avec des spécifications pour les fichiers joints dans les spécifications ebXML (www.ebxml.org) . Cela aboutira à une norme ouverte et globale permettant de transmettre des messages électroniques sur Internet de manière fiable.

Les spécifications de messages ebXML comprennent elles-mêmes un jeu de services et de protocoles qui permet à un client de demander des services aux serveurs au moyen de protocoles de transport au niveau des applications couramment utilisés, notamment le Simple Mail Transfer Protocol (SMTP), l'Hyper Text Transfer Protocol (HTTP) et d'autres. L'ebXML permet de transmettre un message de nature générale comportant un message d'en-tête supportant plusieurs champs de données, tout en prévoyant des signatures numériques à l'intérieur et entre les messages numériques répondant à toute spécification.

Les messages EDIFACT/ONU prévoient la transmission de signatures numériques pour accompagner les messages électroniques. Les messages EDIFACT/ONU prévoient en outre l'utilisation de clés publiques à l'importation et à l'exportation (dans le format de message UNEDIFACT KEYMAN). Comme pour les autres formes de messages, les administrations pourraient souhaiter examiner les questions liées à l'enregistrement et à l'archivage des messages, de manière à préserver la sécurité des données et à gérer les répercussions d'une éventuelle répudiation.

11.9.7 Autorité de certification et cadre légal

Après avoir opté pour une solution reposant sur l'ICP, l'administration des douanes doit examiner plusieurs questions de nature technique et juridique liées à la mise en œuvre de l'ICP. Comme indiqué dans la définition ci-dessus, l'ICP requiert un système pour produire et tenir à jour les certificats numériques, tâches qui incombent généralement à une Autorité de certification. Il s'agit d'une entité qui atteste de l'identité d'une personne ou d'une organisation.

L'Autorité de certification a pour principale fonction de vérifier l'identité des parties et d'émettre des certificats prouvant cette identité. Les certificats numériques constituent un moyen de vérifier l'identité d'une personne (ou d'une entreprise). Ces certificats sont les équivalents numériques des cartes d'identité qui confèrent aux transactions sur Internet les caractéristiques sécuritaires nécessaires.

Le cadre légal existant dans le pays aux fins de l'ICP, qui spécifie les conditions à remplir sur le plan technique et juridique, a une incidence importante

- sur la manière dont les certificats numériques sont émis par une autorité de certification;
- sur la manière dont l'autorité de certification doit gérer la durée de vie d'un certificat;
- sur les normes techniques dont la législation doit encourager le respect; etc.

Pour obtenir un cadre légal type, les administrations peuvent se reporter aux directives présentées à ce sujet dans la législation type de la CNUDCI (http://www.uncitral.org/french/texts/electcom - Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation 2001).

Ce cadre légal peut notamment couvrir :

- la manière dont les informations numériques doivent être authentifiées au moyen d'une signature numérique et la recevabilité de telles signatures en tant qu'éléments de preuve devant les tribunaux
- le processus de création d'une signature numérique
- le processus de vérification d'une signature numérique la convivialité
- les normes techniques applicables aux processus ci-dessus
- la manière dont les autorités de certification seront agréées
- les directives applicables en matière de sécurité au fonctionnement d'une autorité de certification.

En l'absence de tout cadre légal global et général, les administrations pourraient envisager de conclure avec les usagers et les prestataires de services des accords bipartites ou tripartites semblables à ceux qui sont fréquemment conclus dans l'environnement RVA, mais en tenant compte de la plateforme technique reposant sur l'ICP.

11.9.8 L'ICP et la douane : principales questions à examiner

Les administrations peuvent étudier si elles sont en mesure de remplir les fonctions d'une autorité de certification ou si une autre institution publique/officielle ou privée offre des services de certification d'une qualité acceptable. Il existe à cet égard, selon les pays, des modèles différents dans le cadre desquels les autorités de certification peuvent fonctionner, conformément au cadre légal en vigueur, en tant que chaînes (ou hiérarchies) de confiance. Quel que soit le modèle choisi, et l'autorité de certification choisie, plusieurs points devront sans doute faire l'objet d'une décision, parallèlement à l'acceptation des certificats numériques émis par l'autorité de certification.

Appendice A de la partie 10

Exemples de motifs juridiques de répudiation dans le cadre de poursuites judiciaires engagées en Australie

1.0 Poursuites pénales

1.1 Manquement de nature judiciaire (c'est probablement la cause la plus courante de carence dans les poursuites pénales) : absence d'éléments de preuve suffisamment persuasifs (défaut d'inscription dans les registres, d'archivage, etc.) ou non-recevabilité des éléments de preuve (problèmes liés aux travaux d'enquête ou de recueil des éléments de preuve, ou problèmes juridiques liés à la recevabilité des dossiers informatiques).

1.2 Absence d'élément subjectif : de nature individuelle (applicable aux infractions de nature générale telles que fraude – peut ne pas s'appliquer aux infractions à la législation de certaines entités, par exemple à la Loi sur les douanes); ou de nature collective – le cas échéant, l'intention collective doit être déduite de l'intention/comportement des fonctionnaires et des agents. (Client individuel seulement) Moyens de protection du consommateur tels que Loi de la Nouvelle-Galles du sud sur l'examen des contrats. (Lorsque le client est une organisation) Le représentant/agent individuel a agi sans autorisation. Vol d'identité (comme sous 1.5). Le client est mineur d'âge ou ne jouit pas de la capacité à conclure un contrat.

1.3 Moyens de défense tels qu'aliénation mentale ou automatisme (cas peu probable dans ce contexte).

1.4 Le défendeur est mineur en matière de responsabilité pénale (10 ans en Nouvelle-Galles du Sud) (cas peu probable – signe d'un manquement grave en matière de preuve de l'identité)

1.5 Prétendu vol d'identité (intervenu même si un processus approprié de preuve de l'identité/enregistrement a été mis en oeuvre).

2. POURSUITES CIVILES

(Remarque : les exemples ci-après concernent le cas d'un contrat conclu entre une agence et un client. D'autres poursuites peuvent être engagées au civil, par exemple, un courrier électronique donnant de mauvais conseils entraîne une action en responsabilité délictuelle pour fausse déclaration par négligence, mais ce cas est peu probable dans le cadre des transactions avec la douane).

2.1 Défaut d'établissement d'un contrat contraignant (absence de processus d'achat au clic) ou éléments de preuve insuffisants d'un tel processus, notamment :

- fait que le processus ne démontre pas assez clairement l'accord du client
- fait que les termes et les modalités ne sont pas suffisamment indiqués.

2.2 Défaut d'établissement d'un contrat contraignant pour des motifs non liés au processus, notamment absence de considération ou d'intention de créer des relations légales. Peut également comprendre les moyens permettant une rescision sans faute, par exemple erreur réciproque (mais cas peu probable).

2.3 Méfait commis par le destinataire (ou dans certains cas, par un tiers). Divers moyens permettent à un tribunal de contester une transaction, notamment la contrainte (de nature physique ou économique), comportement indélicat, pratiques dolosives ou comportement trompeur (TPA s.52), Yerkey v. Jones, etc.

2.4 (Client individuel seulement) Moyens de protection du consommateur tels que Loi de la Nouvelle-Galles du sud sur l'examen des contrats.

2.5 (Lorsque le client est une organisation) Le représentant/agent individuel a agi sans autorisation.

2.6 Vol d'identité (comme sous 1.5).

11.9.9 Gestion de l'identité

[Proposition d'insertion dans le Chapitre 11, en tant que nouvelle Section 11.10]

La gestion de l'identité consiste à vérifier l'identité d'une entité qui cherche à obtenir un accès à distance à un système informatique, revendique la paternité d'une communication électronique ou signe un document électronique. Dans les systèmes informatiques, les

identités en ligne sont 'électroniques'. Lors d'interactions en face-à-face, l'identité est vérifiée en s'assurant visuellement des attributs qui lui sont liés. De la même façon, les identités électroniques en ligne doivent être vérifiées avec soin avant d'autoriser une personne ou une identité à participer à des transactions par voie électronique. La Section 11.6 évoque les questions relatives aux garanties de l'identité. Il est toutefois nécessaire de traiter les problèmes posés en matière de sécurité et de commerce par l'utilisation opérationnelle d'identités électroniques et la présente section évoque les problèmes de gestion des identités électroniques du point de vue de leur cycle de vie.

L'usage généralisé de la TIC a conduit à une multiplication des applications et des réseaux internes. Pour accéder à une application ou à un réseau, un système spécifique d'identification et d'authentification doit être utilisé. Au fil du temps, de nombreux systèmes d'identité, souvent incompatibles entre eux, tendent à se développer. Les utilisateurs des TIC ne sont pas capables de gérer une multiplicité d'identités électroniques et peuvent ne pas parvenir à préserver des mots de passe de qualité, tels que décrits plus tôt dans le présent Chapitre. Ils vont ainsi accumuler de nombreux mots de passe, ce qui rendra d'autant plus difficile la gestion des comptes et des mots de passe, compliquera le processus d'authentification et entraînera un nombre excessif de comptes d'utilisateurs inactifs et orphelins. Ce scenario produira immanquablement des carences en termes de sécurité et de contrôle, les systèmes informatiques étant ainsi exposés au vol de mots de passe et à leur exploitation à des fins criminelles. Les principes et les pratiques de la Gestion de l'identité visent à apporter des solutions en vue d'une gestion courante des identités électroniques dans un environnement où les utilisateurs doivent pouvoir accéder à de nombreuses applications.

L'OCDE définit comme suit la Gestion de l'identité:

" La Gestion de l'identité numérique désigne l'ensemble des règles, procédures et éléments techniques requis pour mettre en œuvre la politique d'une organisation en ce qui concerne la création, l'utilisation et l'échange d'informations d'identité numérique pour l'accès à des services ou des ressources. Pour être efficaces, les politiques de GIN doivent protéger l'information d'identité numérique tout au long de son cycle de vie – depuis l'enregistrement jusqu'à la révocation – tout en maximisant les gains potentiels liés à son utilisation, notamment entre différents domaines pour la prestation de services intégrés sur l'Internet.

["Le rôle de la gestion de l'identité numérique dans l'économie internet : guide d'introduction à l'intention des décideurs" (juin 2009), Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée].

La gestion de l'identité est un élément important de la sécurité informatique. Elle contribue à traiter les problèmes suivants :

elle offre un contrôle de l'accès matériel et logique aux systèmes informatiques. C'est grâce à ces contrôles qu'il est possible de garantir que seules les personnes autorisées accèdent aux données pertinentes et exécutent sur ces données les opérations autorisées.

elle protège les personnes de tout accès non autorisé à des renseignements personnels et du vol de l'identité lors de l'usage en ligne des identités électroniques. Ces personnes veulent être certaines que leurs identités électroniques ne seront pas employées

de manière impropre ou compromises quand elles sont utilisées dans des transactions électroniques. La Gestion de l'identité contribue donc à protéger leur vie privée en ligne.

Dans un contexte de croissance rapide des services en ligne, les personnes ont du mal à gérer les procédures d'accès définies séparément par chaque service. Par exemple, la nécessité de mémoriser et d'utiliser des identifiants et des mots de passe distincts pour chaque service est fastidieuse et risquée par nature. Pour les prestataires du service, la difficulté réside dans le fait que, les personnes devant être identifiées pour chaque service en ligne, leurs renseignements personnels se démultiplient sur chacun des différents services informatiques, ce qui ouvre la voie à d'éventuelles violations des données et des responsabilités afférentes.

La Gestion de l'identité comprend deux processus principaux, à savoir l'identification (identifier la personne) et l'authentification (vérifier que la personne est bien celle qu'elle prétend être). L'identification consiste à associer la personne à des attributs qui la caractérisent. Ces attributs se présentent sous la forme de renseignements de base sur la personne. Ils peuvent être d'ordre physique (caractéristiques biologiques) ou documentaire (documents attribués ou associés à la personne, par exemple un passeport ou une carte d'identité). Les attributs qui aident à distinguer les personnes entre elles contribuent à les identifier efficacement et les attributs correspondant à une seule personne sont des "identifiants uniques". Le processus de saisie des renseignements sur l'identité est appelé "inscription". L'inscription est un processus en une étape permettant de vérifier ou de prouver l'identité d'une personne. L'objet de l'inscription est de pouvoir utiliser ultérieurement les renseignements aux fins de l'authentification. Le niveau de garantie qu'offre le processus d'identification augmente avec le nombre et la variété des attributs recueillis. Dans ce cas cependant, le risque d'une utilisation impropre des données personnelles et privées recueillies lors de l'inscription est d'autant plus grand. Moins il y a d'attributs recueillis lors de l'inscription et plus le risque de violation de la vie privée est faible.

La vérification des attributs recueillis peut s'effectuer en ligne (par une confirmation visuelle que les attributs correspondent à la personne à identifier) ou hors ligne (en envoyant un numéro personnel d'identification par courrier recommandé). L'exactitude des renseignements personnels recueillis dépend de la fiabilité des données et de la personne ou du système chargé(e) d'évaluer la validité de l'attribut. Des renseignements personnels comme la taille peuvent être évalués de manière fiable et ne sont pas censés varier. En revanche, la vérification d'empreintes digitales dépend de la précision du système d'enregistrement de l'attribut et de la vérification ultérieure. La vérification varie en fonction du type de renseignement sur l'identité à vérifier, de son origine, des processus de vérification mis en œuvre et de la précision du système de vérification.

Le processus d'identification se conclut par la délivrance d'identifiants (Mot de passe utilisateur, jetons d'authentification, etc.). Certains de ces identifiants reposent sur les attributs biologiques des personnes.

Les services d'annuaire servent à stocker et à gérer les comptes, les renseignements sur l'identité et les identifiants d'accès. En l'absence de systèmes 'd'identité fédérée', les renseignements sur les identifiants sont conservés dans des annuaires distincts et destinés à des applications distinctes. La fédération des identités permettrait de tenir à jour plus facilement les politiques de gestion des droits associés aux identifiants électroniques. Les

activités liées à la gestion du compte utilisateur, à la gestion du cycle de vie de l'identité et à la gestion de l'accès s'en trouvent considérablement simplifiées.

La gestion de l'identité fédérée implique des 'parties tierces' qui sont chargées de la gestion des comptes, de l'authentification et de la gestion de l'accès. Grâce aux solutions d'identité fédérée, les utilisateurs ne sont plus submergés par une multiplicité d'identifiants et de mots de passe. La solution de gestion de l'identité par une partie tierce tient lieu de bureau unique pour l'utilisateur et pour le système auquel il accède. La partie tierce est le "fournisseur d'identité", l'utilisateur est le 'sujet' qui souhaite accéder au système informatique d'un gouvernement ou d'une entreprise : c'est la "partie se fiant au certificat". Il n'est pas nécessaire que la partie tierce soit une entité commerciale différente mais son rôle est clairement distinct. Les solutions de gestion de l'identité fédérée comportent des risques juridiques, comme la perte de données à caractère privé impliquant un accès non autorisé aux attributs de l'identité de l'utilisateur. La compromission des renseignements figurant sur la carte d'identité de l'utilisateur peut entraîner des risques d'authentification erronée ou d'accès non autorisé et exposer aux sanctions encourues pour avoir pénétré dans un système par effraction. Il convient de réduire ces risques en prenant les contre-mesures qui s'imposent.

En conclusion, les présentes Directives invitent les administrations des douanes à appliquer des solutions et des principes sûrs pour la Gestion de l'identité, afin d'améliorer la sécurité et de réduire le temps perdu en activités improductives liées à la gestion des utilisateurs.

12. QUESTIONS JURIDIQUES

(Norme 7.4)

12.1 Introduction

Il est impossible de donner des orientations précises en ce qui concerne les questions juridiques qui se posent aux administrations des douanes, car chacune d'elle fonctionne sur des bases et dans le cadre de systèmes juridiques différents. Les orientations fournies ici doivent permettre au lecteur de comprendre globalement les questions juridiques les plus courantes. Il y a lieu de solliciter dès les premières étapes d'un projet le concours d'experts compétents en ce qui concerne les implications juridiques de l'informatisation des procédures douanières.

S'agissant des questions juridiques, il importe peut-être de rappeler que les lois n'ont pas toutes le même champ d'application, il en est ainsi des :

- Conventions internationales (Convention de Kyoto révisée par exemple) ;
- lois supranationales (par exemple, la législation communautaire qui est susceptible d'être appliquée en l'état et qui prévaut sur les dispositions nationales);
- lois nationales d'application générale, qui sont susceptibles de s'appliquer à la douane mais également dans d'autres domaines (par exemple, les lois sur la protection de la vie privée, les lois sur le commerce électronique, les lois sur les signatures numériques, la loi sur la protection des données);
- lois nationales spécifiques, par exemple, la législation douanière nationale qui ne s'applique qu'aux questions relevant de la douane; et des
- lois sur les régimes douaniers qui se limitent à un régime douanier particulier (une loi pourrait par exemple régir le transit douanier).

Les questions juridiques sont parfois citées comme autant d'obstacles insurmontables à la mise en œuvre de certaines solutions informatiques. Un nombre croissant d'administrations membres ont toutefois constaté que la modification des prescriptions juridiques n'est pas nécessairement un processus complexe et long.

12.2 La législation en vigueur est-elle adéquate ?

Lorsqu'un régime douanier est appelé à être informatisé, la majeure partie de la législation en vigueur pourra vraisemblablement demeurer inchangée. Toutefois, l'information entraîne parfois la simplification d'un régime et cette simplification doit le cas échéant être traduite dans le droit. Il peut s'avérer nécessaire de modifier la définition des responsabilités, y compris le moment auquel le paiement doit être effectué, auquel il est estimé qu'une déclaration a été déposée, etc.

12.3 Types de questions juridiques

Dans un environnement informatique, les questions à prendre en considération du point de vue juridique, lors de la mise en place d'un nouveau système, peuvent être regroupées, par exemple, dans les catégories ci-après. Il est à noter que ce type de

regroupement est toujours artificiel et n'est proposé qu'aux fins de l'exposé. Dans la pratique, ces regroupements ne présentent aucune valeur juridique et les questions citées sont susceptibles de relever de plusieurs catégories en même temps.

- Les questions juridiques liées à l'EDI (prescriptions concernant la forme, par exemple, dispositions exigeant l'utilisation de papier, de documents, de documents signés, etc., ou l'utilisation et la recevabilité comme preuve de données électroniques)
- Les questions juridiques liées à la sécurité (la forme et les supports s'agissant du stockage des données, l'identification, l'intégrité, la non-répudiation, la reconnaissance, etc. ainsi que les questions relatives à la preuve)
- Les questions juridiques liées à la protection des données (les restrictions concernant l'accès aux données, les échanges de données entre administrations etc.)
- D'autres questions, par exemple : la confidentialité, les responsabilités et obligations opérationnelles résultant de l'utilisation de systèmes d'échanges de données informatisés, les dispositions en matière de recours, les dispositions juridiques interdisant le cryptage, etc.
- Les modalités d'introduction du nouveau système : par voie d'accord (par exemple, au moyen d'un accord concernant les échanges de données, ce qui soulève des questions contractuelles) ou en prenant les dispositions contraignantes, compte tenu de l'autorité dont l'administration est investie.

12.4 Signature

Même s'il existe des systèmes d'échange de données perfectionnés, les procédures d'importation/d'exportation continuent parfois de reposer, ne fut-ce que partiellement, sur les documents imprimés, et ce en raison des prescriptions juridiques et d'impératifs fonctionnels propres à l'autorité douanière du pays concerné. Dans certains systèmes de TI de la douane, les prescriptions en matière de signature exigent que des déclarations imprimées soient communiquées à la douane outre les données communiquées électroniquement, ce qui empêche l'avènement d'un environnement dématérialisé. Si l'on veut profiter pleinement des avantages qu'offre l'informatique douanière, ces obstacles juridiques doivent être surmontés.

Il existe des techniques efficaces pouvant remplacer une signature manuscrite dans le cadre d'un système informatique douanier. Les mots de passe, les numéros d'identification personnels, les cartes et badges d'identité, etc. ainsi que des signatures numériques sont autant de moyens d'authentifier un message électronique et d'en déterminer l'origine. Ces solutions sont couramment utilisées dans d'autres secteurs tels que la banque ainsi que dans un nombre croissant d'administrations des douanes.

La législation en matière de signature électronique peut obéir à deux logiques, elle peut :

- Préciser expressément les moyens techniques à utiliser (par exemple, quel algorithme, ses modalités d'application, etc.); ou
- Préciser que le choix d'un moyen adapté incombe à la douane.

La seconde solution offre l'avantage de n'appeler aucune modification de la législation en vigueur si la douane souhaite changer de mécanisme.

12.5 Recevabilité

Des obstacles juridiques existent également en ce qui concerne la recevabilité en justice des données lisibles par ordinateur. Dans une résolution adoptée en 1986, l'OMD invite ses administrations membres à faire pression sur les autorités nationales compétentes pour que soient apportées à la loi les modifications indispensables pour que les données lisibles par ordinateur deviennent non seulement recevables comme moyens de preuve devant les tribunaux mais qu'elles puissent être identifiées par des moyens autres que la signature manuscrite (voir le paragraphe 11.4 ci-dessus). Ces réformes juridiques sont indispensables non seulement du point de vue de la douane mais également d'une manière générale pour tous les opérateurs commerciaux.

Lorsqu'une telle législation a été introduite ou est en voie de l'être, il importe de veiller à ce que le système informatique puisse fournir les éléments de preuve nécessaires conformément aux prescriptions en la matière.

12.6 Protection des données et protection de la vie privée

A l'exclusion, en général, des systèmes de lutte contre la fraude, la législation en matière de protection des données et de protection de la vie privée s'applique habituellement aux systèmes de TI de la douane. Son champ d'application peut se limiter aux personnes physiques ou englober tant les personnes physiques que les personnes morales.

Lors de l'élaboration de la législation sur la protection de la vie privée ou la protection des données, la douane doit, dans la mesure du possible, veiller à ce que les dispositions de ladite législation n'hypothèquent pas sa capacité à protéger les intérêts de l'Etat en matière de recettes, de commerce ou autre, en limitant les prescriptions lui permettant de conserver des renseignements et d'échanger des renseignements avec les autres parties concernées (à l'échelon national ou international). La protection de la vie privée devient une question importante lorsque la douane utilise les réseaux de communication publique, comme l'Internet et partage des renseignements sur ses usagers avec des tiers.

Il est également dans l'intérêt du pays concerné que la douane soit habilitée à consulter les systèmes informatiques des opérateurs commerciaux pour procéder aux vérifications/audits nécessaires. La douane doit veiller à ce que la nouvelle législation ne lui interdise pas cette pratique.

Au moment d'introduire une nouvelle technologie d'IC, il faut examiner la législation en matière de protection de la vie privée et de protection des données pour s'assurer que le nouveau système en respecte toutes les dispositions.

Les documents suivants contiennent des données supplémentaires concernant les bases juridiques sur lesquelles reposent les échanges sans support papier.

1) Loi-type de la CNUDCI sur les signatures électroniques et du Guide pour son incorporation 2001 [Nations Unies, 2002]

2) Convention des Nations Unies concernant l'utilisation des communications électroniques dans les contrats internationaux [Nations Unies, 2007]

3) « Promouvoir la confiance dans le commerce électronique : questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques » [Nations Unies, 2007]

13. AUDITS DES CONTROLES INTERNES DES SYSTEMES INFORMATIQUES

(Norme transitoire 6.9)

13.1 Généralités

L'audit d'un système informatique garantit le bon déroulement d'une activité ou d'une procédure déterminée. Ainsi que l'indique l'expression elle-même, l'audit de système consiste à examiner le cycle de traitement dans son intégralité et non pas simplement les transactions proprement dites. Un audit de système ne repose ni sur la vérification rétrospective d'une procédure tangible ni sur l'examen approfondi de la totalité ou d'un nombre significatif des transactions, contrairement à ce qui se fait dans un système manuel, pour s'assurer du bon fonctionnement d'une application ou d'une installation particulière. En revanche, un audit de système vise à renforcer la confiance des utilisateurs en s'appuyant sur les caractéristiques propres au traitement informatique.

S'il peut être établi que la procédure est en soi fiable et précise, et que les dispositifs de contrôle auxquels elle répond sont efficaces et respectés, il est justifié d'en conclure que le résultat présente la qualité escomptée. Le grand avantage des systèmes informatiques, qui est aussi, paradoxalement, leur point faible, est qu'une fois programmés, ils accomplissent systématiquement la même tâche de la même manière, jusqu'à ce qu'une modification soit apportée. Ainsi, s'ils ont été programmés correctement, le résultat sera toujours exact, mais dans le cas contraire, il sera toujours erroné !

La douane peut appliquer les techniques d'audit de système soit aux systèmes des opérateurs commerciaux, soit à ses propres applications internes. Le recours à ces techniques permet de vérifier l'intégrité des systèmes et, le cas échéant, de repérer les points faibles auxquels il faut remédier pour rétablir la confiance. La section qui suit est consacrée à l'audit des systèmes de la douane.

13.2 Audits de conception

Les audits des systèmes informatiques sont particulièrement utiles lors de la conception d'une nouvelle application. S'agissant de la douane, il sera toujours nécessaire de mettre en œuvre de nouvelles applications le plus rapidement possible, en raison de l'introduction d'une nouvelle législation. Toutefois, lorsque la rapidité de la mise en œuvre a été privilégiée, c'est au détriment de la possibilité de procéder facilement à des audits, laquelle a été négligée ou envisagée seulement partiellement. Une mauvaise adaptation du système aux audits se traduit par des contrôles inadéquats, voire inexistants; ce qui est préjudiciable à la fiabilité des données.

C'est pourquoi l'équipe chargée de planifier la mise en œuvre de toute nouvelle application devrait idéalement comprendre un auditeur informatique. Celui-ci sera en mesure de veiller à ce que la question des contrôles et des vérifications rétrospectives ne soit pas négligée. Il pourra également fournir des données d'essai permettant de procéder à

des mises à l'essai réalistes du système. Il sera ainsi par la suite en mesure de confirmer que le traitement des données, depuis leur saisie jusqu'à leur enregistrement définitif, se déroule correctement, et de procéder également à une vérification rétrospective des transactions. Dès lors, si les impératifs en matière d'audit sont pris en considération dès la conception du système, les audits et contrôles ultérieurs n'en seront que plus efficaces et fiables. Il est également plus rentable d'aménager le système à cet effet dès le début, plutôt que de tenter de le faire ultérieurement.

Les principales parties d'un audit de système sont décrites ci-après.

13.3 Planification

La planification est déterminante pour l'efficacité et la crédibilité d'un audit. Elle définit des orientations et précise la portée de l'audit ou l'objectif final au regard duquel l'efficacité de celui-ci sera appréciée. S'agissant des nouveaux systèmes, la planification est généralement précédée d'une étude de faisabilité. La question fondamentale à laquelle la planification doit permettre de répondre est la suivante : est-ce possible ?

La planification permettra donc notamment de déterminer :

- les objectifs de l'audit; l'auditeur doit avoir une idée précise de l'objectif de sa mission. Cet objectif doit également être parfaitement connu des fonctionnaires concernés ou des collaborateurs faisant partie de l'équipe de conception;
- la portée; elle définit les limites de l'audit en précisant les domaines et les systèmes qu'il devra couvrir;
- l'existence de risques; il s'agit de définir les domaines dans lesquels une défaillance aurait des conséquences graves, voire catastrophiques, et sur lesquels l'auditeur doit concentrer ses efforts;
- la conduite de l'audit et l'organisation des entretiens de début et de fin d'audit avec les fonctionnaires concernés; ces réunions permettent de fixer au préalable les règles de base de l'audit et d'écarter ainsi tout risque éventuel de malentendu ou de problème au cours de l'audit proprement dit; elles permettent également aux fonctionnaires concernés de savoir ce qu'ils peuvent attendre des conclusions de l'audit;
- la durée de l'audit; la période sur laquelle s'étalera l'audit doit être définie pour permettre aux fonctionnaires concernés d'organiser leurs travaux en conséquence;
- les ressources nécessaires pour entreprendre l'audit; il est indispensable d'arrêter le nombre d'auditeurs en fonction de la taille du ou des systèmes à analyser, de leur emplacement, ainsi que de la disponibilité des fonctionnaires directement intéressés;
- la période pendant laquelle les fonctionnaires directement intéressés seront disponibles pour des entretiens; il est encore plus essentiel de s'assurer que les fonctionnaires directement intéressés savent parfaitement quand doit avoir lieu l'audit et quand les auditeurs voudront s'entretenir avec eux. Il faut donc dans la mesure du possible s'accorder sur les dates suffisamment à l'avance.

Enfin, il convient que les auditeurs évaluent l'incidence qu'ont eue sur les connaissances acquises à l'issue d'audits antérieurs les modifications apportées éventuellement par la suite au système ou à l'administration qui l'exploite. S'agissant des systèmes existants, de nombreux renseignements ayant été recueillis au cours d'audits

antérieurs peuvent vraisemblablement aider l'auditeur à comprendre le système et la manière dont il a fonctionné par le passé. Toutefois, si de nombreuses modifications ont été apportées, l'utilité de ces renseignements s'en trouve fortement réduite.

13.4 Enquête ou recueil de renseignements

Il existe dans ce domaine un ensemble de méthodes, qui sont essentiellement les suivantes :

13.4.1 Entretiens

Il y a lieu de s'entretenir si possible avec les fonctionnaires d'encadrement de tout niveau tant les utilisateurs des applications que les informaticiens et les concepteurs du système. Grâce à ces entretiens, l'auditeur pourra déterminer :

- la manière dont le fonctionnement du système est perçue (généralement par la direction)
- la manière dont le système fonctionne effectivement (point de vue des utilisateurs)
- la manière dont le système est censé fonctionner (cahier des charges établi par les concepteurs/les utilisateurs)

13.4.2 Examen de la documentation

Les auditeurs peuvent examiner :

- le cahier des charges des utilisateurs qui précise les tâches que les utilisateurs souhaitent que le système accomplisse;
- le descriptif du système qui précise la solution proposée par l'équipe de conception;
- les rapports d'essais, qui consignent, entre autres, la gamme et la portée des essais afin de garantir l'efficacité d'un système en toutes circonstances, sa précision, sa solidité et de s'assurer qu'il dispose de la capacité nécessaire pour faire face à des surcharges inattendues, et enfin, qu'il est doté de dispositifs nécessaires pour déceler et signaler les erreurs;
- les conclusions des essais et des exploitations en parallèle : ces rapports consignent les résultats des exploitations en temps réel d'un site pilote ou en parallèle avec un système existant;
- les manuels d'utilisation : ces manuels doivent être faciles à comprendre et exhaustifs;
- les mesures de secours/de sécurité : ces mesures doivent préciser comment remédier aux défaillances et la manière de protéger le système tant au niveau des applications que du matériel;
- la politique d'archivage : cette politique doit définir la fréquence des copies de sauvegarde ainsi que la durée de la conservation et le lieu d'entreposage de ces copies; en l'occurrence, elles doivent être entreposées à l'écart du site et dans un coffre à l'épreuve du feu.

Ces éléments, qui ne sont pas exhaustifs, permettent de déterminer les contrôles, internes ou opérationnels, qui ont été mis en œuvre ou qui font défaut. Les auditeurs peuvent également tirer de nombreuses conclusions de l'état (voire de l'absence) de la documentation relative au système qui peut, par exemple, être dépassée ou incomplète.

L'examen de la gestion de la configuration et des documents fournira aux auditeurs d'autres indices sur le bon fonctionnement du système et sur la confiance qu'il inspire.

13.5 Consignation des résultats d'un audit

Les auditeurs consigneront leurs conclusions soit dans un rapport écrit, soit sous forme de diagrammes. Il existe de nombreuses conventions et normes en matière d'établissement des organigrammes, chacune d'elles étant généralement destinée à rendre compte d'un aspect particulier. A cet égard notamment :

- l'organigramme de programmation
- l'organigramme d'analyse
- les schémas fonctionnels
- les schémas de bases de données.

Les auditeurs compareront souvent leurs propres organigrammes avec celui du système à l'examen pour déceler toute omission ou anomalie. Les appendices 5 et 6 contiennent des exemples courants de diagrammes de ce type. A ce stade de l'audit, et avant de passer à l'étape suivante, la personne ou l'organisation faisant l'objet de l'audit confirme que l'auditeur a appréhendé correctement le système.

13.6 Evaluation

En évaluant les renseignements recueillis, l'auditeur peut commencer à déterminer les points faibles réels ou supposés des contrôles internes. Cette partie de sa mission permettra à l'auditeur d'élaborer des essais et de déterminer les domaines dans lesquels ceux-ci doivent être appliqués, afin d'apprécier l'efficacité des contrôles et la fiabilité du résultat.

13.7 Confirmation des conclusions d'un audit

Cette procédure vient conclure chaque étape d'un audit. La confirmation peut intervenir, par voie d'observation, au stade du recueil des renseignements, ou à celui de l'évaluation. On peut procéder par inspection des dossiers, des rapports de résultats, etc., voire en exécutant à nouveau la procédure de traitement.

L'examen de la documentation, qu'elle soit générée par ordinateur ou qu'il s'agisse de dossiers concernant les transactions établis par voie manuelle, devra confirmer dans quelle mesure elle est exhaustive, exacte et fiable. Lorsqu'une vérification rétrospective est possible, celle-ci sera entreprise pour s'assurer que la chaîne ne comprend aucune interruption.

Lorsqu'il est impossible de procéder à une vérification rétrospective, soit par manque d'éléments, soit en raison du volume des transactions, les TIC peuvent apporter des solutions, par exemple l'élaboration de programmes spéciaux pour examiner les données enregistrées sur un support magnétique. De tels programmes peuvent être écrits de manière ad hoc dans le même langage que celui du logiciel d'application ; on peut également utiliser des logiciels d'interrogation de fichiers propres à un constructeur.

Ces méthodes permettent de manière simple de vérifier et de confirmer les totaux des transactions, la liquidation des droits, des remises, etc. Elles peuvent également servir à tester des combinaisons de données inhabituelles, ce qui serait pratiquement impossible à l'aide de techniques manuelles. Bien souvent, les auditeurs installent sur le système un ensemble de programmes d'essai et de logiciels d'audit pouvant être mis en oeuvre à chaque audit. Ces logiciels peuvent être modifiés, par exemple en modifiant certains paramètres, mais ne sont réellement utiles que lorsque le système demeure inchangé.

Ces moyens perfectionnés sont essentiellement utilisés lorsque des erreurs éventuelles pourraient avoir des conséquences importantes, par exemple, compromettre gravement l'acquittement des droits et taxes dus ou fausser les statistiques, entraînant de la sorte des problèmes de balance des paiements, etc.

13.8 Rapport

A l'issue de l'audit, les auditeurs adresseront généralement à la direction un rapport contenant des recommandations sur la manière dont les lacunes peuvent être éliminées et les contrôles adaptés pour les rendre plus efficaces. Des contrôles peuvent même être rejetés s'ils semblent inadéquats dans une situation particulière.

Les recommandations ne sont en rien contraignantes mais leur rejet éventuel est généralement précédé d'un examen approfondi, puisqu'il pourrait, dans certaines circonstances, avoir des conséquences désastreuses.

13.9 Vérification après audit

Lorsqu'un nouveau système a été installé ou qu'un système existant a été remanié substantiellement, il est habituel d'en vérifier le fonctionnement. Cette vérification, réalisée après un certain délai, vise à déterminer si le système fonctionne comme prévu, s'il présente des points faibles ou si des enseignements peuvent en être tirés en vue de projets futurs. De même, lorsque suite à l'audit d'un système informatique, des recommandations concrètes ont été formulées concernant son fonctionnement, une vérification après audit permettra de déterminer si ces recommandations ont été exécutées et d'en apprécier les répercussions; lorsque les recommandations n'ont pas été mises en œuvre, il y a lieu d'en déterminer la raison.

13.10 Conclusion

Lorsqu'un système a été enregistré et évalué et que les modifications recommandées pour améliorer le contrôle ont été mises en œuvre, on peut légitimement s'attendre à ce que le système fonctionne de manière fiable jusqu'au prochain remaniement important. Il conviendra de procéder à des audits périodiques qui devront confirmer que la situation est demeurée inchangée et que les contrôles qui ont été incorporés dans le système continuent à être mis en œuvre et respectés.

14. PROBLEMES COURANTS

14.1 Introduction

Avant de mettre en œuvre un système informatique quel qu'il soit, il convient d'examiner les domaines susceptibles de poser des problèmes lors de l'exécution du projet et de définir des stratégies garantissant que les problèmes éventuels, qu'ils soient propres à l'organisation administrative, aux procédures ou aux ressources, ne provoquent pas l'échec du projet.

Il faut prévoir un soutien lorsqu'un système informatique est installé dans une administration des douanes. Les administrations qui envisagent de s'informatiser souhaiteront peut-être également mettre en place un service pour appuyer les mesures qu'elles prennent. Toutes les activités et les coûts y relatifs imputables à la gestion des activités liées aux technologies de l'information, la conception, la mise au point et l'emploi de systèmes informatiques nouveaux ou améliorés et l'exploitation, l'entretien et le soutien de ces systèmes revêtent une grande importance et il faut en tenir compte (voir l'appendice 8 : Tableau récapitulatif des travaux successifs à entreprendre).

14.2 Résistance culturelle

Les fonctionnaires des douanes peuvent craindre que l'informatique ne menace leurs emplois et opposer une résistance à son introduction. Les administrations des douanes peuvent éliminer ces résistances et rendre leurs fonctionnaires plus productifs en organisant des programmes de formation et d'incitation. Elles peuvent également combattre les rumeurs et calmer les incertitudes en veillant à ce que les renseignements nécessaires concernant les plans, la portée, etc., du projet soient accessibles à tout un chacun, et ce dès le début du projet. A cet égard, une solution consiste à publier à intervalles réguliers des rapports sur le projet et à organiser des réunions avec le personnel le plus directement touché.

14.3 Informatisation des données de base

Si les données de base ne sont pas informatisées, l'intérêt que présente l'informatisation pour certains partenaires de la douane s'en trouve réduit. Par exemple, lorsque les documents commerciaux ne sont pas communiqués par voie électronique, les entreprises ne peuvent pas les utiliser pour établir leurs déclarations en douane. Une solution consiste à charger des bureaux de services de saisir les données. Ces bureaux peuvent être gérés, soit par la douane, soit par des entreprises privées. Dans ce dernier cas, le bureau de services doit être supervisé par la douane pour garantir que les normes en matière de saisie satisfont aux critères en la matière. Une autre solution consiste à acquérir le matériel dont les entreprises et la douane ont besoin par l'intermédiaire de programmes de crédits fournisseurs, ce qui permettrait éventuellement d'obtenir des remises substantielles.

14.4 Absence d'infrastructure adéquate

Un autre problème qui risque d'hypothéquer l'informatisation est l'absence d'infrastructures de télécommunication adéquates. Le cas échéant, les données peuvent être échangées au moyen de disquettes plutôt que par l'intermédiaire des réseaux publics. Il faut également examiner la possibilité d'utiliser la communication par satellite. Il peut également être difficile pour certaines administrations d'avoir accès à une source ininterrompue d'approvisionnement en électricité. Lorsque les systèmes informatiques doivent être disponibles en permanence, il faut inscrire l'achat d'un générateur électrique au budget du projet.

14.5 Législation douanière

L'amendement par trop fréquent de la législation douanière risque également d'empêcher l'informatisation globale de la douane dans le cadre d'un seul et même projet. Plutôt que d'informatiser la totalité d'un système appelé à devenir rapidement obsolète, il est préférable d'adopter une démarche modulaire en informatisant les diverses activités et en les ajoutant à un système central, selon les besoins ou la permanence de la législation. On peut citer en exemple le système de paiement et de recouvrement des droits, auquel d'autres systèmes pourraient être ajoutés ultérieurement. Des ressources peuvent également être consacrées à la rationalisation des procédés manuels en vigueur afin d'éliminer tout chevauchement dans le système.

14.6 Limitation des ressources et des compétences

Lorsque les ressources sont limitées, il importe de définir les priorités du projet en fonction des gains de productivité et d'efficacité, de manière à tirer le meilleur parti possible des crédits engagés. Par exemple, une administration pourrait envisager d'informatiser en premier lieu la procédure la plus coûteuse en main d'oeuvre afin d'améliorer sa productivité. Une administration des douanes peut ne pas posséder les compétences nécessaires pour mettre en oeuvre un projet. Lorsque la solution consistant à engager des spécialités externes est envisagée, il importe de planifier correctement les coûts et, peut-être surtout, de définir expressément le rôle du ou des consultants.

APPENDICE 1 - STRUCTURES DE L'INFORMATION ET DES TELECOMMUNICATIONS POUR LE COMMERCE ELECTRONIQUE

A propos du commerce électronique

En quoi consiste le commerce électronique ? Aux fins de la présente partie, le commerce électronique est défini comme le «processus consistant à échanger des renseignements par voie électronique en vue de faciliter le commerce des biens et des services. Une composante essentielle de ce processus est l'intégration des procédures du commerce aux technologies appropriées».

L'expression «commerce électronique» ayant commencé à être utilisée relativement récemment, d'aucuns pensent qu'il s'agit d'un nouveau moyen d'effectuer des transactions. Toutefois, de nombreuses administrations, dont la douane, utilisent déjà des aspects du «commerce électronique» dans leurs méthodes de travail actuelles. Les partenaires commerciaux échangent habituellement des renseignements par voie électronique au moyen de l'EDI, du courrier électronique, de télécopies, etc. Le «commerce électronique» consiste essentiellement à effectuer des transactions par voie électronique. Il pourrait être défini de manière plus formelle comme «un moyen d'effectuer des transactions en utilisant les techniques des télécommunications et de l'informatique aux fins des échanges de données entre des systèmes d'information automatisés indépendants».

Le commerce électronique couvre certes l'EDI, mais va également au-delà puisqu'il comprend toutes les autres technologies existantes susceptibles d'être utilisées pour transmettre des renseignements d'un partenaire commercial à un autre. Il importe de rappeler que les renseignements se composent de données structurées (utilisant des formats de messages normalisés, le transfert direct des enregistrements d'une base de données, des codes-barres), d'images (image et textes non structurés) et de sons (messagerie vocale, etc.). Les administrations des douanes doivent aujourd'hui examiner l'incidence que pourraient avoir ces autres techniques sur leurs opérations. Elles doivent notamment déterminer si l'utilisation de ces techniques peut leur fournir des solutions plus rentables, leur permettre d'offrir plus aisément des services plus souples aux entreprises et aux autres administrations publiques avec lesquelles elles peuvent avoir besoin d'échanger des renseignements.

Le commerce électronique est déjà bien implanté au sein de la douane. Les administrations utilisent plus largement les techniques de l'EDI aux fins du dédouanement des marchandises à l'importation et à l'exportation. La communication à grande échelle de renseignements de nature commerciale et de données figurant sur les déclarations de marchandises entre les entreprises et la douane se prête également à l'application des techniques de l'EDI. Cette application du commerce électronique prendra sans doute de plus en plus d'ampleur au cours des dix années à venir. Toutefois, dans la mesure où le rôle de la douane s'élargit et où de nouveaux moyens de réaliser les tâches traditionnelles apparaissent, il deviendra de plus en plus nécessaire d'exploiter certaines autres possibilités offertes par l'utilisation du commerce électronique au sens le plus large.

L'expression « commerce électronique » est employée comme une expression générique décrivant diverses relations électroniques, qui présentent toutes leurs propres règles et caractéristiques. Parmi les nombreuses configurations possibles, il convient de signaler les relations entreprises-consommateurs (B2C), entreprises-entreprises (B2B) et les trois types de relations impliquant le gouvernement, à savoir le gouvernement-entreprises (G2B), gouvernement-citoyens (G2C) et gouvernement-gouvernement (G2G).

Voies électroniques d'accès

Le schéma ci-dessous offre un résumé des différentes voies d'accès qui peuvent être fournies à l'utilisateur des services proposés par la douane dans le cadre du commerce électronique.

Normes d'échange d'informations

Normes d'échange d'informations dans le Modèle de données de l'OMD – Il s'agit ici de se concentrer sur la signification sémantique de haut niveau des données et sur la manière de pourvoir à l'interaction entre le gouvernement et les entreprises. On recense trois niveaux d'abstraction en ce qui concerne un modèle de données, qui peut ainsi être externe, physique et conceptuel. Le Modèle de données de l'OMD s'attache au niveau d'abstraction le plus élevé, à savoir le niveau conceptuel du modèle de données.

Le Modèle de données de l'OMD en tant que Modèle de données conceptuel

Les modèles les moins abstraits, appelés modèles externes, décrivent les mises en œuvre spécifiques d'une déclaration de marchandises ainsi que le signalement d'un manifeste. Les exemples les plus représentatifs sont le message CUSCAR conforme à la version 3 du MD de l'OMD et le message GOVCBR, conforme à la Version 3.0 du Modèle de données de l'OMD.

Les modèles physiques sont plus généraux parce qu'ils décrivent un jeu ou une catégorie d'exemples mais saisissent encore la technologie dans laquelle les exemples ont été mis en œuvre. Le guide de mise en œuvre des messages (MIG) est un exemple représentatif de mise en œuvre d'un message CUSCAR qui est inclus dans la version 1.1 du Modèle de données de l'OMD qui a été publié en novembre 2003.

Les modèles conceptuels suppriment la technologie de mise en œuvre pour souligner les concepts et les significations définissant certaines catégories d'exemples de documents. Le niveau d'abstraction le plus élevé a été intégré depuis peu à la version 2.0 du MDD. Les exemples les plus représentatifs sont les diagrammes de catégorie UML pour tous les types de documents, les diagrammes de catégorie UML pour une seule catégorie de documents et l'inventaire des 450 éléments de données appelés collectivement jeux de données MDD.

Nécessité du modèle conceptuel

A l'instar de la plupart des milieux commerciaux, les milieux douaniers n'évoluent pas au même rythme que la technologie. Si le Modèle de données de l'OMD est uniquement décrit comme une technologie spécifique (à savoir, à travers un modèle de données physiques tel qu'EDIFACT), il sera nécessaire de définir le Modèle de données dans chaque technologie

future. En tout état de cause, il sera difficile, voire impossible, de garantir que tous les modèles de données physiques sont analogues dans les différentes technologies.

En établissant un modèle conceptuel et en saisissant toutes les règles commerciales dans le modèle conceptuel, les milieux commerciaux pourront mettre en œuvre les documents douaniers quelle que soit la technologie utilisée (à savoir les modèles de données physiques) satisfaisant leurs besoins.

Autres avantages liés à l'établissement d'un modèle conceptuel

On gagnerait en clarté parce que la signification et les règles de présentation d'un élément de données sont préservées dans différents modèles physiques qui sont dérivés d'un modèle conceptuel unique. Par exemple, la catégorie «TransportEquipment» désigne les ''ressources matérielles nécessaires pour contenir ou retenir le(s) envoi(s) devant être transporté(s)'' et comporte les mêmes attributs de catégorie que la catégorie soit utilisée dans une déclaration à l'entrée, une déclaration à la sortie, une déclaration de fret à la sortie, une déclaration de fret à l'entrée, une déclaration de transport ou une déclaration de transit.

L'interopérabilité avec les modèles de données des autres administrations ou des administrations nationales participantes et des entreprises est facilitée quand chaque élément des renseignements est doté d'une signification unique dans l'ensemble des documents douaniers. Par exemple, le terme «TransportEquipment» de l'ONU/CEFACT, qui appartient au domaine du transport, peut être directement réparti dans la catégorie «TransportEquipment» du Modèle de données de l'OMD.

Dans la Version 3.0, les avantages de l'élaboration d'un modèle conceptuel sont visibles. Depuis la publication de la Version 3.3, le Modèle de données de l'OMD se divise en deux parties :

1) Les composantes normalisées (le Jeu de données, les modèles d'informations, les modèles de procédures opérationnelles et les listes de codes) et

2) Les Dossiers d'information (Directives de mise en œuvre du message et Schémas XML traduisant les modèles d'échange électronique de données adaptés aux besoins des activités).

Un « Dossier d'information » indique comment les composantes normalisées du Modèle de données de l'OMD ont été regroupées et sont utilisées pour répondre aux besoins d'une activité donnée. Les Dossiers d'information contiennent surtout les modèles pour l'échange de données électroniques mais ils peuvent également être employés pour expliquer la signification opérationnelle que recouvrent les informations structurées utilisées lors de l'échange d'informations. Les Dossiers d'information étaient auparavant appelés les " Messages électroniques". Ces modèles sont de différents types et concernent notamment les déclarations propres aux réglementations transfrontières (importation, exportation, rapport de chargement à l'importation, rapport de chargement à l'exportation, déclaration de transit, etc.), les Réponses Gouvernement-entreprises et les échanges Gouvernement-Gouvernement.

En outre, les licences, les permis, les certificats et les autres types d'échanges du "guichet unique" ont été incorporés à la Version 3.3.

On peut considérer que les Dossiers d'Information du Modèle de données disposent d'une structure hiérarchisée. Les Dossiers d'information de base de l'OMD comprennent les principaux schémas transactionnels dans un environnement de Guichet unique, et notamment :

- Les messages entreprises-gouvernement tels que IM (Déclaration d'importation des marchandises), EX (Déclaration d'exportation des marchandises), CRI (Rapport de chargement à l'importation), CRE (Rapport de chargement à l'exportation), CONV (Rapport sur le moyen de transport), les renseignements préalables TRT (Transit), etc.;
- Les messages gouvernement-entreprises tels que les messages de notification de la mainlevée ou de statut de la Déclaration ;
- Les messages entre toutes les parties concernant les licences, les certificats, les permis et autres types d'autorisation ;
- Les messages gouvernement-gouvernement concernant la gestion de la garantie aux fins des admissions temporaires et d'autres types d'échanges.

Les Dossiers d'information de base contiennent le maximum des données exigées dans un contexte donné d'utilisation. À partir de ces Dossiers, l'EPMD s'est employée dans le cadre de ses travaux sur le soutien à la mise en œuvre à élaborer les formats couramment employés, formats qu'elle a nommés « Dossiers dérivés d'information de l'OMD ». En règle générale, ces « Dossiers dérivés d'information » reposent sur des modèles électroniques normalisés appliqués à l'échelon international, comme par exemple les formulaires électroniques FAL de l'Organisation maritime internationale (OMI), le Document administratif unique de l'UE, les permis électroniques CITES, la Déclaration de valeur de l'OMC, la Gestion de la garantie dans le contexte du Carnet TIR, etc.

Les Membres et les autres organisations qui utilisent déjà le Modèle de données pour des échanges réels de données ou qui sont en passe de le mettre en œuvre peuvent même aller plus loin dans la « personnalisation » locale et élaborer un dossier intitulé "Mon Dossier d'information". Ce dossier, qui contient des informations très spécifiques, vise à décrire la manière dont chaque composante du Modèle de données de l'OMD a été adoptée et utilisée dans les contextes opérationnels particuliers d'une mise en œuvre donnée. Il peut être élaboré plus facilement à partir d'un « Dossier dérivé d'information » similaire. Par exemple, un Membre utilisant un formulaire de déclaration en douane basé sur le « Document administratif unique » peut élaborer le document intitulé « Mon dossier d'information » à partir du Dossier dérivé d'information publié par l'OMD. De même, un Membre peut élaborer un dossier « Mon dossier d'information » couvrant les exigences nationales applicables au rapport de chargement.

Un tel dossier permet d'expliquer comment les exigences nationales sont liées aux formulaires FAL de l'OMI ainsi qu'au Modèle de données de l'OMD.

L'élaboration d'un dossier intitulé « Mon dossier d'information » reviendrait aux Membres et aux organisations qui utilisent le Modèle de données de l'OMD. L'EPMD s'efforce de déterminer comment un usage national de l'OMD peut être représenté dans un modèle XML standard de l'OMD pouvant être « lu par une machine ». Un tel modèle permettrait non seulement de dresser un tableau comparatif de l'usage national des différents éléments du Jeu de données de l'OMD mais aussi de copier automatiquement les données d'un dossier « Mon dossier d'information » dans les outils d'un prestataire de solutions, facilitant ainsi une introduction plus rapide de solutions concrètes pour l'échange de données.

Echange d'informations : un paysage qui évolue

Dans les scénarios antérieurs de l'EDI, ces informations sont fournies à la douane par le biais de normes internationales de messages telles que :

- CUSDEC : message douanier EDIFACT/ONU concernant la déclaration en douane;
- CUSCAR : message douanier EDIFACT/ONU concernant la cargaison;
- CUSREP : message douanier EDIFACT/ONU concernant le moyen de transport;
- CUSRES : message douanier EDIFACT/ONU concernant la réponse de la douane ; et
- CUSEXP : message douanier EDIFACT/ONU concernant les envois express.

Il existe actuellement en matière d'EDI plusieurs autres messages internationaux EDIFACT/ONU pouvant servir aux fins ci-dessus. A titre d'exemple, on peut citer le CUSDEC et le GESMES (statistiques), le PAXLST (liste des membres d'équipage/des voyageurs) et le SANCRT (impératifs divers en matière de licences et de certificats).

A ce jour, le Modèle de données de l'OMD comprend un message EDIFACT GOVCBR, couvrant l'essentiel des données exigées par les organismes chargés de la réglementation des flux transfrontières. Une administration pourrait ainsi utiliser le message GOVCBR pour répondre à toutes ses exigences liées aux messages plutôt que de tenir à jour plusieurs messages EDIFACT pour y répartir ces exigences.

Modèles de transaction :

L'échange de renseignements avec les opérateurs commerciaux passe par le recours à différents modèles de transaction (basés sur une taxinomie ebXML). Ces modèles sont les suivants :

i) Faire une offre – Accepter une offre :

[Exemple : la douane accepte un opérateur commercial sur son application Internet en lui proposant un cahier des charges. L'opérateur commercial accepte ce cahier des charges.

ii) Demander une information – Fournir une information. [Exemple : L'opérateur commercial demande des informations sur les droits et taxes liés à un article qu'il souhaite importer. La douane fournit les informations demandées.]

iii) Demander une confirmation – Recevoir une réponse de confirmation (ou un refus). [Exemple 1 : L'opérateur commercial soumet une déclaration en vue de la mainlevée des marchandises. La douane confirme ou infirme la mainlevée des marchandises. Exemple 2 : L'entreprise transmet une caution et demande confirmation de l'enregistrement de ladite caution. La douane enregistre la caution et transmet la confirmation.]

iv) Formuler une demande – Recevoir une réponse. [Exemple : La douane formule auprès de l'opérateur commercial une demande de précisions concernant la nature du produit importé et reçoit une réponse.]

v) Délivrer une notification à un opérateur commercial. [La douane envoie à l'opérateur commercial une notification concernant le statut de son compte fiscal.]

vi) Fournir des informations personnalisées aux opérateurs commerciaux [La douane informe tous les opérateurs commerciaux du statut de leurs marchandises respectives.]

Grâce à Internet et aux techniques du commerce électronique, et en se conformant aux modèles de transaction décrits ci-dessus, il est facile de permettre aux entreprises d'avoir accès uniquement à leur domaine dans les bases de données de la douane. Ces renseignements peuvent être fournis grâce à la technique de publication des bases de données. En général, les renseignements suivants pourront être consultés :

- Base de données dans lesquelles sont saisies les entreprises (solde des garanties en cours, nom et coordonnées de l'intéressé)
- Messages administratifs (renseignements concernant les modifications du système, les mises à jour, etc.);
- Situation des marchandises faisant l'objet de la déclaration du partenaire commercial (mainlevée accordée, marchandises retenues pour vérification, demande de renseignements complémentaires);
- Taux des droits antidumping/droits compensatoires;
- Statistiques en matière d'erreurs;
- Taux de change;
- Base de données sur les tarifs (nomenclature et renseignements concernant les listes tarifaires harmonisées);
- Contingents;
- Codes de région/district/bureau de douane;
- Codes de pays;
- Codes des bureaux de douane à l'étranger
- Montant et situation en ce qui concerne le remboursement
- Amendes et pénalités infligées par la douane (acquittées sur une période déterminée)
- Renseignements tarifaires contraignants (pour les marchandises importées ou exportées).

Toutefois, avant que ces renseignements ne soient rendus accessibles, un certain nombre de questions doivent être résolues, par exemple en ce qui concerne les droits d'auteur, la confidentialité, la protection des données et le paiement éventuel de redevances.

S'agissant des renseignements mis à la disposition des usagers, la question des droits d'auteur est particulièrement importante, notamment en ce qui concerne des documents tels que les listes tarifaires harmonisées. Chaque administration membre devra examiner si elle a le droit de publier des listes tarifaires à jour. La douane devrait également s'assurer qu'elle est autorisée à publier les renseignements fournis par d'autres administrations. L'Internet permettra d'établir un lien entre le site web de la douane et celui des autres secteurs publics.

La question du prélèvement et du recouvrement de redevances au titre de la mise à disposition de certains renseignements devra également être examinée. Par exemple, la plupart des administrations nationales demandent aux milieux commerciaux une contribution financière pour disposer de leurs listes tarifaires et des mises à jour y afférentes. Dans un univers informatisé, les administrations devront déterminer si une telle redevance doit être demandée. Avant de diffuser gratuitement des renseignements, la douane doit tenir compte de leur origine et déterminer si leur propriétaire les diffuse habituellement contre paiement.

La question de la confidentialité et de la protection des données doit être traitée de manière adéquate, tout en autorisant l'accès aux bases de données de la douane. Les données nominatives et les données commerciales soumises à la douane à titre confidentiel sont soumises aux dispositions de la législation nationale sur la confidentialité et la protection des données.

L'efficacité du contrôle des marchandises et des voyageurs peut également être améliorée en autorisant la douane à accéder aux bases de données des opérateurs commerciaux. Par exemple, lorsque la douane peut consulter la base de données des voyageurs d'une compagnie aérienne, elle est mieux à même de déterminer quels sont les voyageurs devant faire l'objet d'un contrôle supplémentaire à leur arrivée. De même, en consultant la base de données d'un transporteur, la douane peut déterminer les envois à haut risque.

Codes

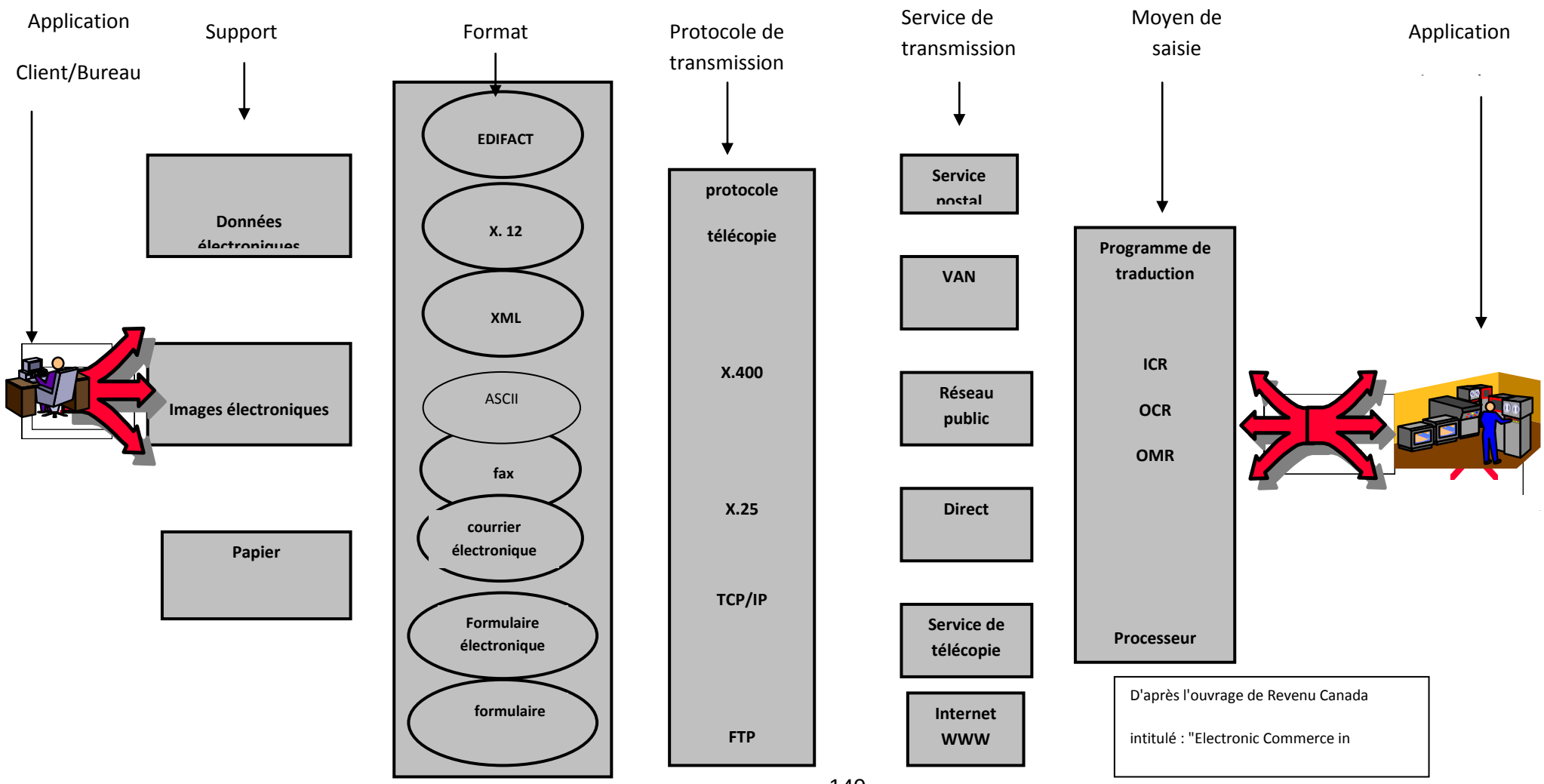
(Normes 3.11 et 7.2)

Lors des échanges d'informations, les codes et les identificateurs jouent un rôle très important. L'OMD recommande d'utiliser des codes internationaux, tels que les codes de pays et de devises ISO, les codes de transport ONU, le Système harmonisé de désignation et de codification des marchandises de l'OMD, etc. (voir l'Appendice 9). L'utilisation des codes internationaux existants, garantit l'ouverture et l'accessibilité des systèmes douaniers. L'utilisation harmonisée de codes au niveau des applications contribuera de manière significative à faciliter le commerce international. Elle contribuera à simplifier la mise au point des systèmes des entreprises et des autres administrations qui souhaitent communiquer avec la douane. Elle rendra également les échanges de renseignements entre administrations des douanes plus avantageux.

Recommandations

La douane devra mettre en place les mécanismes nécessaires en matière de consultation avec les milieux commerciaux ainsi que les capacités indispensables en matière d'opérations, de ressources humaines et d'infrastructure des systèmes d'information pour utiliser efficacement le commerce électronique. En premier lieu, l'administration des douanes devra connaître avec précision ses capacités internes ainsi que les attentes des parties extérieures, ce qui exige une consultation au sein des différents services de l'administration et avec les parties extérieures qui participeront éventuellement au commerce électronique avec l'administration. En second lieu, après examen des répercussions sur le plan juridique et politique, l'administration des douanes devra définir sa stratégie en matière de commerce électronique et élaborer un plan de mise en oeuvre qui sera approuvé par les cadres supérieurs et les parties extérieures concernées. Enfin, la douane devrait s'efforcer d'aligner ses exigences sur le Modèle de données de l'OMD et élaborer au niveau national des dossiers intitulés "Mon Dossier d'information", offrant ainsi la transparence nécessaire pour réduire les coûts des activités commerciales.

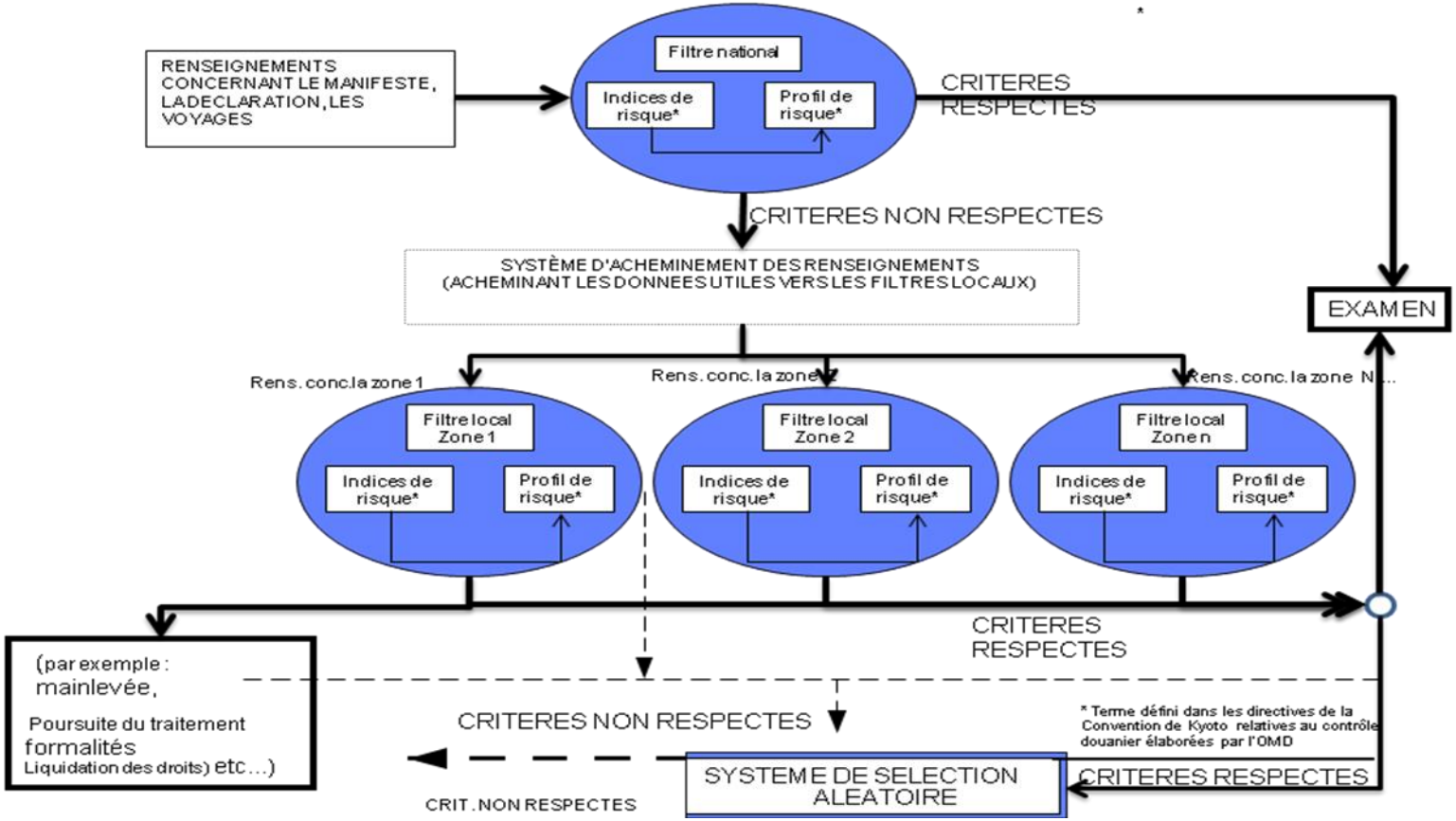
APPENDICE 2 - STRUCTURES DE L'INFORMATION ET DES TELECOMMUNICATIONS POUR LE COMMERCE ELECTRONIQUE



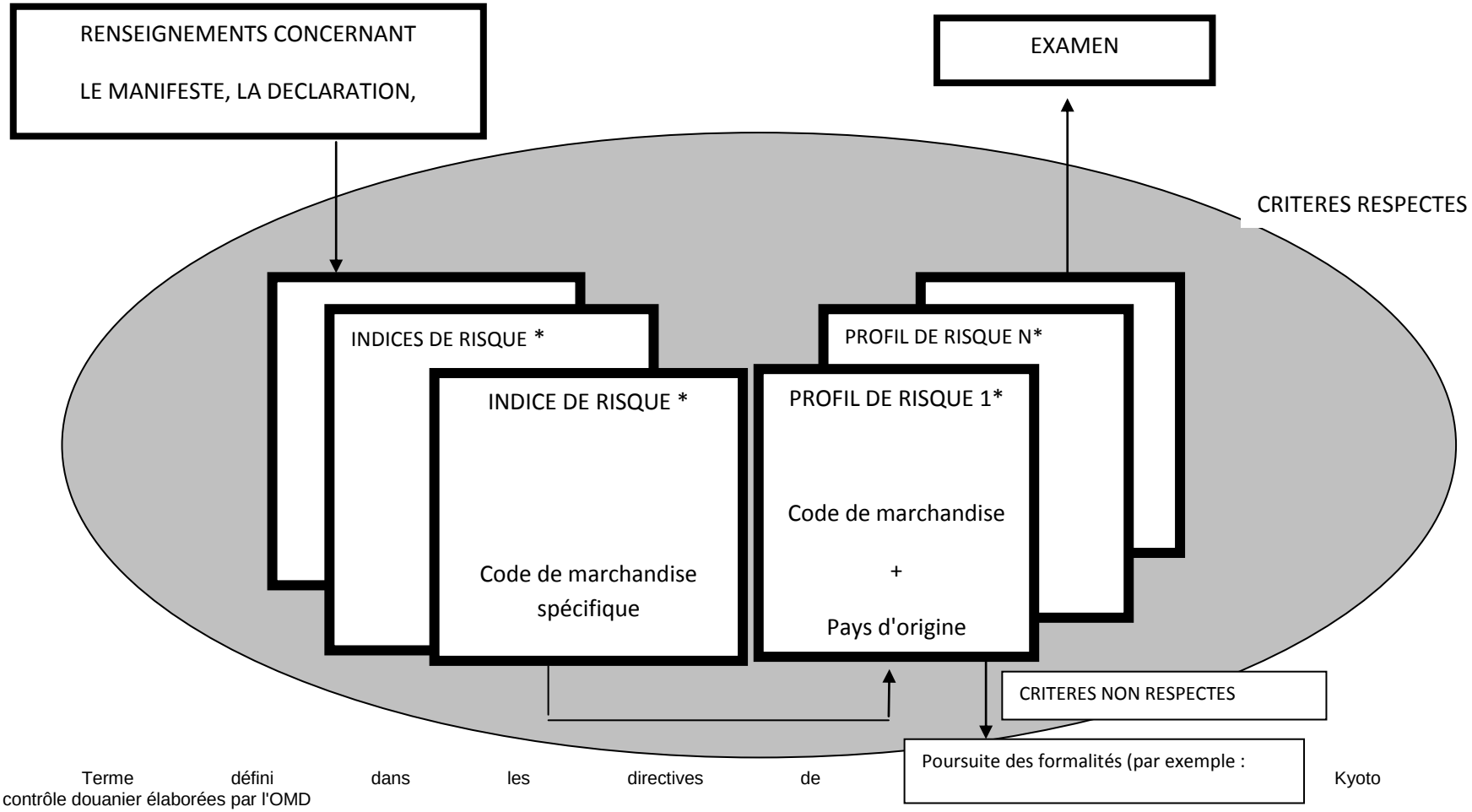
D'après l'ouvrage de Revenu Canada

intitulé : "Electronic Commerce in

APPENDICE 3 - PROCEDE DE SELECTION LOCAL

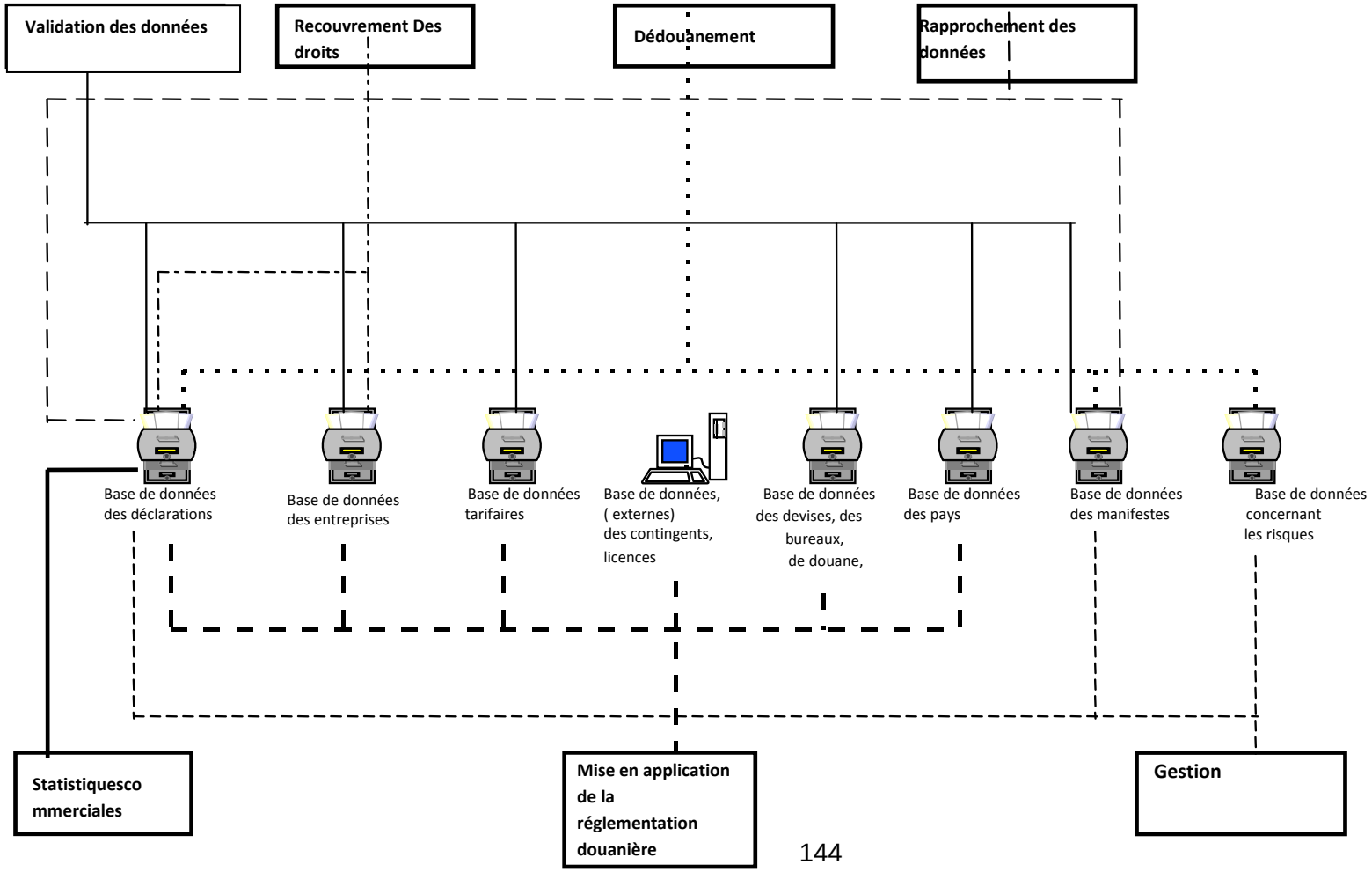


APPENDICE 4- SYSTEME DE FILTRE DES PROFILS DE SELECTION



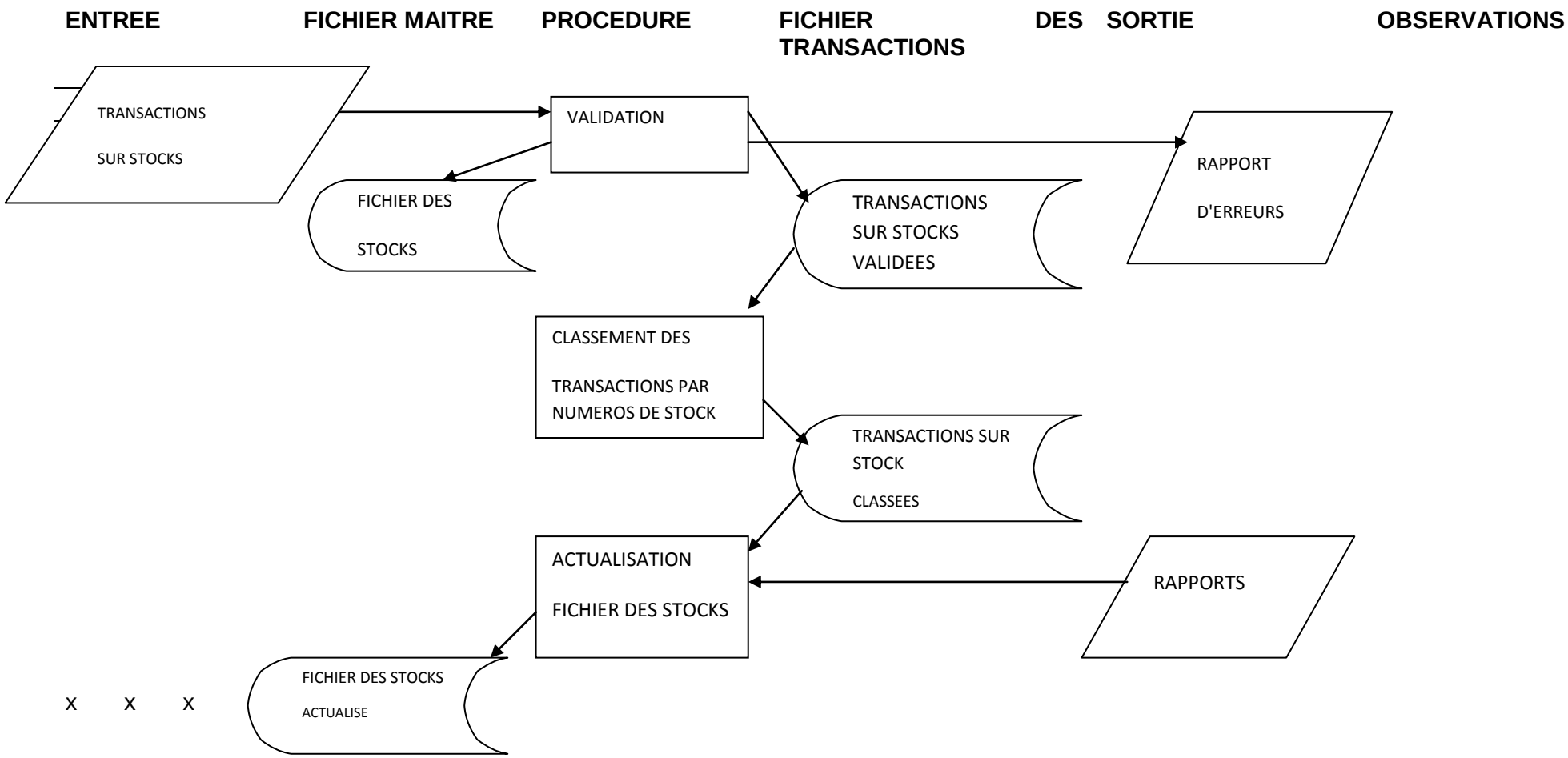
* Terme défini dans les directives de Kyoto relatives au contrôle douanier élaborées par l'OMD
.

APPENDICE 5 - MODÈLE DE PROCÉDURES DOUANIÈRES ET D'EXPLOITATION DES FICHIERS



Blank page

APPENDICE 6 - DIAGRAMME DE TRAITEMENT PAR ORDINATEUR



x x x

APPENDICE 7 – Glossaire des termes et abréviations

ADO	Voir "Architecture de documents ouverte".
Application	Programme ou ensemble de programmes élaborés pour répondre à un besoin particulier de l'utilisateur.
Architecture de documents ouverte	Architecture permettant de procéder à des "échanges aveugles". C'est-à-dire que deux systèmes peuvent échanger des documents tout en conservant la présentation et la "révisabilité" de ceux-ci, la seule condition préalable étant que les deux systèmes utilisent un profil normalisé particulier de la norme ADO internationale. L'ADO permet d'exploiter la plupart des documents susceptibles d'être utilisés dans une administration.
Base de données	Ensemble de données reliées entre elles enregistré de manière que les utilisateurs autorisés puissent y accéder au moyen de procédures de dialogue simples et conviviales.
Boîte à lettres électronique	Lieu où peuvent être stockés temporairement des paquets de messages avant que la transmission n'en soit poursuivie. Les messages entrants sont stockés dans la boîte à lettres du destinataire et consultés par celui-ci ultérieurement.
Cahier des charges de l'utilisateur	Rapport officiel précisant dans le détail tous les besoins de l'utilisateur d'un système informatique en cours de développement.
Commerce électronique	Moyen d'effectuer des transactions en utilisant la technologie des télécommunications et de l'informatique aux fins des échanges de données entre des systèmes d'information automatisés indépendants.
Contre-mesure	Mesure prise pour remédier à un danger, risque, etc.

Contrôleur de transmission	Unité intelligente accomplissant des fonctions d'interface en ligne telles que détection d'erreurs, synchronisation, par exemple entre un groupe de modems et un ordinateur ou un processeur d'un réseau de communication.
Document	Tout support (y compris les bandes magnétiques et les disquettes, les microfilms et les messages de commerce électronique) destiné à contenir et contenant effectivement des données informatiques enregistrées.
Données de base	Facture, formulaire, souche, justificatif ou tout autre document écrit attestant de la réalité d'une transaction et dont les éléments d'information de base peuvent être extraits pour traitement.
Echange de données informatisé	Transmission par voie électronique entre systèmes informatiques de données structurées conformément à des normes d'élaboration convenue de messages.
Echange de renseignements	Au sens de la présente directive, échange électronique de données entre systèmes informatiques.
EDI	Voir "Echange de données informatisé".
EDIFACT/ONU	Système d'échange de données informatisé pour l'administration, le commerce et le transport, élaboré sous l'égide de l'ONU.
En ligne	Qualifie un système dans lequel des données ou des instructions sont introduits directement au point d'origine et les données de sortie transmises directement à leur destinataire.
Etude de faisabilité	Phase de mise en oeuvre d'un système au cours de laquelle le système proposé est évalué en fonction de considérations d'ordre technique ou financier. C'est suite à cette étude qu'il est décidé de passer ou non à l'étape suivante.

Formulaire électronique	Document contenant certains éléments pré-encodés et dans lequel des données variables doivent être introduites.
GUI	Graphic user interface (voir "interface graphique (GUI)".
HTML	HyperText Markup Language (voir "language HTML").
ICP	Un système ICP est un système informatisé gérant la production, la tenue à jour et l'émission des codes de chiffrement et des signatures numériques. Ces deux types de protection, à savoir le chiffrement et la signature numérique, sont composés de deux éléments : une clé publique à laquelle des tiers peuvent avoir accès et une clé privée qui doit être protégée contre tout accès par des tiers. La clé publique et les éléments d'identification sont enregistrés dans un certificat numérique, signé par l'autorité compétente. La signature numérique de cette autorité sur le certificat en cause lie l'identité de l'usager à sa clé publique. Elle garantit également que la clé publique n'a pas fait l'objet de manipulations frauduleuses.
Identification	Dans le domaine de la sécurité des données, contrôles qui empêchent ou détectent la modification délibérée et/ou la destruction accidentelle de données, y compris l'identité de l'expéditeur et du destinataire d'un message.
Informaticien	Personne qui effectue des opérations sur les données pour atteindre un objectif déterminé.
Intégrité	Protection de programmes ou de données contre toute perte ou altération afin de conserver leur intégrité aux fins de l'exploitation prévue.

Interface graphique (GUI)	Interface de programme utilisant les capacités graphiques d'un ordinateur pour faciliter l'utilisation du programme. Les interfaces graphiques (GUI) bien conçues évitent à l'utilisateur de devoir apprendre des langages de commande complexes. En revanche, de nombreux utilisateurs estiment travailler plus efficacement à l'aide d'une interface pilotée par commandes, notamment lorsqu'ils maîtrisent déjà le langage de commande. Le logiciel Microsoft Windows est une interface graphique (GUI).
Interface informatique	Frontière commune entre deux unités reliées entre elles.
Internet	Réseau informatique international reliant les ordinateurs d'établissements d'enseignement, d'administrations publiques, d'entreprises, etc.
Introduction directe par les entreprises	Système permettant aux déclarants d'introduire eux-mêmes les déclarations dans le système informatique de la douane à partir de terminaux d'ordinaire situés dans leurs propres bureaux ou par l'intermédiaire de réseaux commerciaux appartenant à des tiers.
ISO	Organisation internationale de normalisation
Langage HTML (Langage de balisage hypertexte)	Langage de description de pages utilisé pour créer des pages sur le Web. Les pages sont rédigées en texte normal; des balises HTML sont ensuite posées afin de formater le texte qui peut alors être consulté à l'aide d'un logiciel de navigation sur le WWW. Ces balises comprennent des options de formatage, des renvois à d'autres pages, des graphiques. Le langage HTML n'est pas subordonné à une machine particulière.
Ligne commutée	Ligne de télécommunication permettant à deux ordinateurs de communiquer mais nécessitant de l'expéditeur qu'il compose un numéro de téléphone pour établir la communication entre les deux systèmes.
Ligne spécialisée (louée – dédiée)	Ligne louée par un abonné pour son usage exclusif et permanent.
Logiciel	Programmes, procédures, sous-programmes et éventuellement documents associés au fonctionnement d'un système de traitement de l'information.

Non répudiation	Possibilité d'empêcher l'expéditeur ou le destinataire d'un message de nier l'avoir envoyé ou reçu.
Magasin virtuel	Un magasin qui n'existe pas nécessairement dans la réalité et qui a été créé au moyen de logiciels (sur le WWW par exemple).
Modem	Modulateur -DEModulateur - Appareil qui module le signal émis et démodule le signal reçu. Un modem peut convertir par exemple le signal numérique produit par un ordinateur en un signal analogique à transmettre, habituellement par l'intermédiaire du réseau téléphonique.
Norme internationale	Norme reconnue officiellement à l'échelon mondial par un organisme international de normalisation reconnu (ISO, CEE/ONU, etc.).
Organigramme	Représentation graphique d'un processus (logique ou physique).
Protocole	Ensemble formellement défini de conventions régissant le format et le contrôle des éléments entrant et sortant échangés entre deux systèmes en communication.
Réseau à valeur ajoutée	Service de communication transmettant des données par l'intermédiaire des réseaux des entreprises de télécommunications et proposant des services supplémentaires de traitement des données assurés au moyen de matériel propre. Parmi ces services, on peut citer le stockage temporaire et la communication de messages, l'établissement d'interfaces entre terminaux et centres serveurs.
Réseau de communication	Ensemble de dispositifs de communication reliés entre eux.
Réseau de télécommunications	Voir "Réseau de communication".
RVA (VAN)	Voir "Réseau à valeur ajoutée".
Saisie de données	Enregistrement de données au moyen d'une unité périphérique (un clavier, par exemple).
Schéma de base de données	Carte de la structure logique globale d'une base de données.
Schéma fonctionnel	Schéma d'un système dont les principales parties sont représentées par des figures

	géométriques annotées, destiné à indiquer tant les fonctions des divers éléments que les relations entre eux.
SIG	Voir "système intégré de gestion".
Signature numérique	Texte court, code, etc. propre à un utilisateur ou à un processus, utilisé pour signer les messages transmis au moyen d'un système de communication.
SMIME	Protocole Secure Multipurpose Internet Mail Extension (www.ietf.org/html.charters/smime-charter.html)
SMTP	Protocole Simple Mail Transfer (www.raddist.rad.com/networks/1998/smtp/smtp.htm#SMTP)
Système intégré de gestion (SIG)	Système conçu pour fournir, parfois en temps réel, à la direction et à l'encadrement les renseignements exacts, utiles et opportuns dont il a besoin.
Technologie de l'information et de la communication	Combinaison micro-électronique de moyens informatiques et de télécommunications permettant de gérer, de saisir, de traiter, de stocker et de diffuser des informations sous forme vocale, numérique ou de texte.
TEF	Voir « Transfert électronique de fonds ».
Terminal à écran de visualisation	Dispositif permettant à l'utilisateur d'introduire des données dans un ordinateur au moyen d'un clavier, d'un photostyle ou d'un écran tactile et de visualiser les résultats, le texte ou les graphiques produits par l'ordinateur sur un écran à tube cathodique.
TI	Voir « Technologie de l'information et de la communication ».
TIC	Voir « Technologie de l'information et de la communication ».
Traducteur EDI	Conversion dans un format d'EDI convenu afin de permettre l'envoi et la réception de données présentées dans un format d'application.
Transfert électronique de fonds	Ensemble des techniques informatiques permettant de transférer des fonds d'un compte bancaire à un autre par des moyens électroniques et des échanges de données. Exemples : argent électronique, carte de

	débit, carte de crédit, télérèglement des factures (www.ebilling.org)
Transfert électronique de fonds Sécurité / protocoles / systèmes	Protocole Secure Socket Layer (http://home.netscape.com/eng/ssl3/ssl-toc.html) Transaction électronique sécurisée (www.setco.com) ou (www.setco.org) Paiement électronique (www.I-Pay.com) Micro-paiement (www.w3.org/Ecommerce/Micropayments/#About) Système de portefeuille électronique ouvert (www.PCSCworkgroup.com)
Unité centrale	Unité contenant les circuits qui commandent les instructions et en assume l'exécution.
W W W	Voir "World Wide Web".
World Wide Web	La couche graphique superposée à l'Internet. Alors que l'Internet proprement dit ne contient que du texte, le Web est de nature graphique. Les textes et les images graphiques mémorisés dans les serveurs sont transmis aux logiciels de navigation des usagers par l'intermédiaire du réseau et peuvent alors être visualisés.
XML	Langage de balisage extensible (www.xml.org)
X.21	Protocole d'Interface à usage général entre un équipement terminal de traitement de données (ETTD) et un équipement de terminaison de circuit de données (ETCD) permettant une exploitation synchronisée sur les réseaux publics de commutation de données.
X.25	Protocole d'Interface entre un équipement terminal de traitement de données (ETTD) et un équipement de terminaison de circuits de données (ETCD) destiné aux terminaux fonctionnant en mode de transit par paquets sur les réseaux publics de commutation de données.
X.400	Normes pour les gestionnaires de messages.
X.509	Certificat (voir «ICP») utilisé pour vérifier

certains renseignements échangés sur un réseau (Internet par exemple). Il contient la clé publique du propriétaire des clés, ainsi que des renseignements d'identification servant à confirmer l'identité du propriétaire des clés et de l'émetteur du certificat. Les certificats sont stockés dans des annuaires publiquement accessibles comme les annuaires X.500.

x x x

Appendice 8 - DIAGRAMME FONCTIONNEL DE LA TECHNOLOGIE DE L'INFORMATION

DECLENCHEURS	• Directives du gouvernement et de l'administration des douanes • Evolution dans le secteur de la TI • Attentes internes des usagers • Situation de la force de travail de la TI	• Exigences nouvelles et/ou différentes en matière de prestation de services • Exigences nouvelles et/ou différentes en matière de procédures administratives • Exigences nouvelles et/ou différentes en matière de gestion • Modifications législatives	• Défaillances des systèmes • Besoins de remplacement en matériel & logiciels • Solutions/opportunités technologiques nouvelles et/ou différentes • Demandes/problèmes des utilisateurs

↓ ↓ ↓

ACTIVITES	**GESTION**	**ELABORATION/AMELIORATION**	**MISE EN OEUVRE**	**EXPLOITATION/SOUTIEN**
	• Définition d'une stratégie en matière de TI • Elaboration des programmes opérationnels/ commerciaux • Détermination du budget et des sources de financement • Définition et étude des possibilités technologiques • Elaboration d'un ensemble d'approches de normes & d'outils modernes • Plan anti-sinistre • Surveillance et évaluation	• Planification/gestion de projet • Définition des spécifications commerciales • Détermination des spécifications du système • Conception de l'architecture des données, du réseau, du matériel et des logiciels • Définition des besoins en matière de réseau, matériel & logiciels • Evaluation des options technologiques • Intégration d'un logiciel tiers • Programmation et essai des applications • Définition des processus relatifs aux documents	• Elaborer les spécifications techniques et celles relatives aux utilisateurs techniques • Formation des usagers et des opérateurs • Fourniture, évaluation et mis en place d'une infrastructure et des applications • Migration des applications & des données • Gestion de la mise à jour	• Mise en service/activation des applications • Elaboration & surveiller l'application des accords sur la qualité des service et la rentabilité de la TI • Programmation des opérations du système • Maintien d'une capacité suffisante & d'une utilisation équilibrée • Aide et support technique aux utilisateurs • Recherche et surveillance des problèmes • Réparation/remplacement/ amélioration des composants de l'infrastructure • Maintien d'un niveau de sécurité continu • Restauration après défaillances/sinistre • Gestion des équipements et des données

↓ ↓ ↓ ↓

RESULTATS	• Evaluation des performances • Stratégies & programmes en matière de TI • Main-d'œuvre qualifiée • Normes and pratiques relatives aux politiques	• Architecture mise à jour • Applications nouvelles/modifiées • Infrastructure nouvelle/modifiée	• Contrats relatifs aux produits & services • Formation du personnel et des utilisateurs qualifiés • Projets & exécution de la mise à jour • Mise en œuvre des applications et de l'infrastructure	• Disponibilité des systèmes • Accords sur la qualité du service • Correction des systèmes & résolution des problèmes • Reprise sur incident/sinistre • Référentiels mis à jour		
OBJECTIFS DE LA TI	Satisfaire aux exigences des partenaires & des usagers	Elaborer des produits et services TI de manière rentable et dans les délais prescrits	Permettre une grande disponibilité des systèmes	Tenir à jour une documentation sur l'éthique et la sécurité des informations	Disposer d'une main d'œuvre qualifiée et productive dans le domaine de la TI	Fournir aux usagers des solutions technologiques novatrices
CONTRIBUTION AUX OBJECTIFS COMMERCIAUX DE LA DOUANE	Favorise la fourniture de service, la formation des usagers, le recouvrement des droits, la lutte contre la fraude, la protection des frontières et une gestion saine	Forme un personnel compétent, qualifié et productif	Renforce l'efficacité et la rentabilité des fonctions commerciales et de soutien	Fournit des solutions permettant de réaliser des économies	Garantit le fonctionnement continu des processus informatisés	

x x x

Appendice 9 – Recommandation de l'OMD concernant la TI

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE

CONCERNANT LE

NUMERO DE REFERENCE UNIQUE POUR LES ENVOIS (RUE) A DES FINS DOUANIERES

(30 juin 2001)

LE CONSEIL DE COOPERATION DOUANIERE,

EU EGARD à la mondialisation des échanges commerciaux internationaux

SOUHAITANT contribuer à faciliter le passage en douane des marchandises en trafic international

SOUHAITANT accroître l'efficacité et le rendement des administrations des douanes lors du traitement des transactions commerciales internationales

CONSCIENT de l'importance croissante d'une coopération douanière à l'échelon international visant à garantir un meilleur respect de la législation douanière et à assurer la facilitation des échanges licites

RECOMMANDE que les Membres du Conseil et les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi que les Unions douanières ou économiques adoptent et appliquent un numéro de référence unique pour les envois (RUE) qui devrait :

- être utilisé pour toutes les transactions commerciales internationales;
- servir uniquement de code d'accès pour le contrôle, le repérage des envois, l'information et le rapprochement de renseignements, et ne devrait pas en soi fournir de renseignements au sujet de l'envoi proprement dit ;
- permettre de désigner de manière unique un envoi à l'échelon national et international;
- être appliqué au niveau de l'envoi, celui-ci étant défini comme « le nombre total d'envois figurant sur le contrat de vente entre le vendeur et l'acheteur »;
- être attribué le plus tôt possible par le « vendeur » au cours du déroulement de la transaction internationale; et
- être un numéro de référence à usage douanier pouvant devoir être communiqué à la douane à tout moment au cours de l'accomplissement des formalités douanières.

RECOMMANDE EGALEMENT que le numéro de référence unique pour les envois présente les caractéristiques suivantes :

- longueur maximale de 35 caractères alphanumériques.
- le premier caractère qui indique l'année au cours d'une période de dix ans est un chiffre de 0 à 9. (Il est estimé que la référence de l'envoi revêtirait ainsi un caractère unique dans le temps, ce qui suffirait pour remplir les obligations juridiques applicables en matière de conservation des données aux fins des audits).

- les deux caractères suivants seraient réservés au code ISO alpha-2 de pays et correspondrait au lieu d'origine du vendeur. (Il est estimé que la référence de l'envoi revêtirait ainsi un caractère unique sur le plan géographique, s'agissant du pays).
- les 32 caractères restants constitués par le code de l'entreprise reconnu officiellement à l'échelon national ainsi qu'une référence propre à l'entreprise.

DEMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général de l'OMD la date à laquelle ils appliqueront la présente Recommandation et les conditions de cette application. Le Secrétaire général en informera les administrations des douanes de tous les Membres du Conseil. Il en informera également les administrations des douanes des membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières et économiques qui ont accepté la présente Recommandation.

x x x

Appendice 10 – Recommandation de l'OMD relative à l'utilisation des sites Web par les administrations des douanes

CONSEIL DE COOPERATION DOUANIERE TC2-3855

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'UTILISATION DES SITES SUR LE WORLD WIDE WEB PAR LES ADMINISTRATIONS DES DOUANES
(26 juin 1999)

LE CONSEIL DE COOPERATION DOUANIERE,

DESIREUX de faciliter le passage des biens et personnes à l'échelon international à travers les contrôles douaniers,

DESIREUX de faciliter la diffusion des renseignements concernant les réglementations douanières et d'aider les usagers, notamment les voyageurs et les intervenants dans le commerce international, à accéder à ces renseignements,

CONSIDERANT qu'il est important de mettre les renseignements d'ordre réglementaire pertinents à la disposition du public au moyen d'un système rentable et d'accès facile,

EU EGARD à l'acceptation large de l'Internet et du World Wide Web (WWW) comme moyen de communication et de diffusion de renseignements,

EU EGARD à l'utilisation croissante de l'Internet et du WWW par les administrations des douanes,

RECOMMANDE aux Membres du Conseil et aux Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi qu'aux Unions douanières ou économiques de créer un site douanier sur le World Wide Web pour leur administration,

RECOMMANDE EGALEMENT aux Membres du Conseil et aux Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi qu'aux Unions douanières ou économiques de fournir, par le biais du site Web de leur administration douanière, les données minimales mentionnées en annexe à la présente Recommandation,

INVITE les Membres du Conseil et les Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières ou économiques qui acceptent la présente Recommandation à notifier au Secrétaire général du Conseil la date à laquelle ils appliqueront la Recommandation et les modalités de sa mise en

application. Le Secrétaire général transmettra ces renseignements aux administrations des douanes de tous les Membres du Conseil. Il les transmettra également aux administrations des douanes des Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

Annexe à la Recommandation relative aux sites de la douane sur le Web

Renseignements fondamentaux à inclure dans les sites Web de la douane

Renseignements destinés aux voyageurs

- Présentation sommaire de la douane
- Renseignements détaillés sur les franchises
- Renseignements détaillés sur les prohibitions à l'importation et à l'exportation
- Renseignements sur les circuits douaniers (système du double circuit)
- Pénalités sanctionnant les infractions douanières
- Coordonnées (y compris adresse de courrier électronique) des personnes à contacter pour plus de renseignements
- Liaisons avec les autres sites pertinents, notamment l'immigration et l'agriculture.
- Renseignements disponibles dans plusieurs langues
- Accès aux publications officielles

Renseignements détaillés sur les franchises

Les données relatives aux franchises devraient couvrir tous les produits, y compris les quantités et les valeurs maximales. Des précisions devraient également être fournies sur les conditions d'octroi des franchises comme le lieu de départ du voyageur, la durée du séjour, l'âge du voyageur, etc. Dans certains cas, notamment lorsqu'il s'agit de zones économiques, des franchises différentes sont autorisées suivant le lieu de départ du voyageur et ces différences devraient être clairement indiquées.

Renseignements détaillés sur les prohibitions à l'importation et à l'exportation

Les marchandises soumises à des prohibitions ou des restrictions devraient être clairement signalées, comme les armes et munitions, les animaux vivants, certains types de plantes, l'ivoire, les espèces monétaires, etc. Les pénalités sanctionnant les infractions à la loi devraient également être mentionnées.

Renseignements sur les circuits douaniers (système du double circuit)

Les principaux renseignements sur le fonctionnement du système de double circuit et sur les formalités à accomplir par les voyageurs qui souhaitent déclarer des marchandises à la douane à leur arrivée devraient être fournis, avec des exemples de formulaires à remplir.

Pénalités sanctionnant les infractions douanières

Des renseignements complets devraient être fournis afin d'indiquer aux voyageurs les pénalités qu'ils risquent de se voir infliger en cas de violation délibérée de la législation.

Coordonnées (y compris adresse de courrier électronique) des personnes à contacter pour plus de renseignements

Un point de contact avec la douane, notamment une adresse de courrier électronique publique, serait très utile pour permettre aux usagers d'introduire des demandes précises.

Liaisons avec les autres sites pertinents, notamment ceux de l'immigration et de l'agriculture

Des liaisons avec d'autres sites du gouvernement sur le Web tels que ceux de l'immigration, de l'agriculture et de tourisme, aideraient les visiteurs à recueillir des renseignements complets sur toutes les réglementations à observer lors de l'arrivée dans le pays.

Renseignements disponibles dans plusieurs langues

Le tourisme constitue une part très importante de l'économie de nombreux pays et il est possible qu'un grand nombre de visiteurs ne parlent pas la langue du pays où ils se rendent. L'administration des douanes devrait veiller à ce que les renseignements fournis aux voyageurs soient disponibles dans plusieurs langues.

Accès aux publications officielles

Les différentes publications, brochures, etc. officielles devraient pouvoir être consultées ou commandées par le biais du site sur le Web. Il convient d'être attentif au format des documents disponibles pour téléchargement.

<u>Renseignements destinés aux opérateurs commerciaux</u>

- Présentation sommaire de la douane
- Présentation sommaire de la législation et des régimes douaniers
- Législation nationale, y compris les réglementations douanières applicables à tous les régimes douaniers
- Renseignements sur les droits et les tarifs
- Taux de change
- Renseignements sur les prohibitions et restrictions en vigueur
- Marche à suivre pour remplir une déclaration en douane
- Décisions de classement
- Pénalités sanctionnant les infractions douanières
- Coordonnées des personnes à contacter (y compris adresse de courrier électronique)
- Liaisons avec les autres services gouvernementaux
- Accès aux publications officielles

Présentation sommaire de la législation et des régimes douaniers

Cette rubrique fournira une description sommaire des différents régimes douaniers et de la législation dans le cadre de laquelle ils s'inscrivent. Elle devrait être considérée comme une introduction générale aux activités douanières. Des renvois devraient être prévus vers des explications plus détaillées concernant certains régimes ou certaines parties de la législation nationale.

Législation nationale, y compris les réglementations douanières applicables à tous les régimes douaniers

Les sites Web de la douane doivent contenir les textes de loi relatifs au commerce international (importations, exportations, transit, etc.). Toutefois, dans la plupart des cas, la législation est présentée sous forme d'un texte suivi sans aucun lien hypertexte. Afin que le site soit plus utile pour les milieux commerciaux, des liens hypertextes devraient être créés dans les documents pour signaler les références importantes.

Des moteurs de recherche* par mots clés devraient également être mis à la disposition des utilisateurs du site Web.

Renseignements sur les droits et les tarifs

Les principaux renseignements relatifs au tarif et aux taux de droits applicables aux différents types de marchandises devraient être disponibles. L'accès à une version électronique complète du tarif national serait la solution idéale. Toutefois, une copie papier du tarif devrait au moins être disponible dans un format "pdf" (portable document format). Les opérateurs commerciaux pourraient ainsi télécharger le document afin de le visionner et de l'imprimer.

Taux de change

L'accès à la liste des taux de change officiels devrait être considéré comme une nécessité absolue.

Renseignements sur les prohibitions et les restrictions en vigueur

Des précisions sur les marchandises faisant l'objet de prohibitions ou de restrictions similaires, de contingents, etc. devraient être fournies. Les conditions spéciales auxquelles est subordonnée l'importation ou l'exportation de ces marchandises devraient être clairement indiquées.

Marche à suivre pour remplir une déclaration en douane

Un manuel d'utilisation expliquant comment remplir une déclaration en douane est très utile pour les entreprises et permet d'améliorer la qualité des données introduites dans les systèmes douaniers. La plupart des administrations des douanes disposent déjà de ce type de manuel sur support papier et devraient convertir ce manuel sous une forme (format)

* Logiciel servant à entreprendre des recherches à partir de mots clés dans les documents sur un site Web.

pouvant être placée sur le Web. Un tel "manuel de formation" pourrait être transformé en un programme interactif exhaustif.

Décisions de classement

Les entreprises ont souvent besoin de renseignements sur des questions de classement. Toutes les décisions de classement officielles devraient donc être disponibles sur le site Web de la douane, ce qui rendrait moins nécessaire de s'adresser directement aux fonctionnaires des douanes pour obtenir ce type de renseignement.

Pénalités sanctionnant les infractions douanières

Des renseignements complets devraient être fournis afin d'indiquer aux opérateurs commerciaux les pénalités qu'ils risquent de se voir infliger en cas de violation délibérée de la législation.

Coordonnées des personnes à contacter (y compris adresse de courrier électronique)

Comme pour les voyageurs, les coordonnées (y compris les adresses de courrier électronique) des fonctionnaires des douanes responsables dans les différents domaines devraient être fournies.

Liaisons avec les autres services gouvernementaux

Des liaisons avec d'autres sites Web tels que ceux des Ministères du commerce et des finances et de la Chambre de commerce nationale devraient également être prévues.

Accès aux publications officielles

Les différentes publications, brochures, etc. officielles devraient pouvoir être consultées ou commandées par le biais du site sur le Web. Il convient d'être attentif au format des documents disponibles pour téléchargement.

Création d'applications informatiques sur le Web

Les renseignements mis à la disposition des entreprises et des voyageurs risquent d'être statiques, c'est-à-dire que les personnes qui reçoivent les renseignements peuvent les lire et les imprimer, mais ne peuvent généralement pas les intégrer dans leurs propres applications. Les administrations des douanes devraient envisager la création d'applications interactives pouvant être utilisées indifféremment par les clients extérieurs ou par les membres du personnel douanier.

x

x x

Appendice 11 – Recommandation de l'OMD relative au Guide de l'OMD régissant la répartition des données

CONSEIL DE COOPERATION DOUANIERE

TC2-3845

**RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE*
RELATIVE A L'UTILISATION DU GUIDE DE L'OMD REGISSANT
LA REPARTITION DES DONNEES**

DANS LES MESSAGES DOUANIERS EDIFACT/ONU

(21 juin 1995)

LE CONSEIL DE COOPERATION DOUANIERE,

SOUHAITANT faciliter les échanges internationaux de données entre administrations des douanes et entre les administrations des douanes et les intervenants dans le commerce,

CONSIDERANT que les messages EDIFACT/ONU peuvent être utilisés indépendamment de leur domaine d'application et que le développement de leur utilisation dans le cadre du commerce international facilitera sensiblement les mouvements de marchandises,

CONSIDERANT EN OUTRE qu'il est souhaitable qu'un ensemble de règles adoptées à l'échelon international, universellement applicables et régissant l'utilisation des messages douaniers EDIFACT/ONU soit appliqué a l'Echange de Données Informatisé,

RECOMMANDE que les Membres du Conseil de coopération douanière et tous les Membres de l'Organisation des Nations Unies et de ses institutions spécialisées, ainsi que les Unions douanières ou économiques, adoptent le Guide de l'OMD régissant la répartition des données dans les messages EDIFACT/ONU comme le document de référence normalisé pour le développement de tous les guides d'utilisation des messages EDIFACT/ONU utilisés par les administrations des douanes pour les échanges de données électroniques entre les administrations des douanes et entre celles-ci et les intervenants dans le commerce,

DEMANDE aux Membres du Conseil de coopération douanière et aux Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux

* "Conseil de coopération douanière" (CCD) est le nom officiel de l'Organisation mondiale des douanes (OMD)

Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil de coopération douanière la date et les modalités de sa mise en application. Le Secrétaire général transmettra ces renseignements aux administrations des douanes des Membres du Conseil de coopération douanière. Il les transmettra également aux administrations douanières des Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

x x x

Appendice 12 – Recommandation de l'OMD relative aux données exigées aux fins des RPCV

CONSEIL DE COOPERATION DOUANIERE

TC2-3844

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE

RELATIVE AUX DONNEES EXIGEES AUX FINS

DES RENSEIGNEMENTS PREALABLES CONCERNANT

LES VOYAGEURS (RPCV)

(6 juillet 1993)

LE CONSEIL DE COOPERATION DOUANIERE,

CONSTATANT les risques accrus que présentent les voyageurs aériens, notamment en matière de trafic illicite de drogue,

CONSTATANT l'utilisation croissante de la télématique, tant par les transporteurs que par les autorités douanières, et les avantages que l'emploi de cette technique peut apporter,

RECONNAISSANT que la transmission électronique des données concernant les voyageurs peut accélérer le contrôle desdits voyageurs et s'avérer très avantageuse du point de vue des contrôles douaniers,

TENANT COMPTE de l'Annexe J.1. de la Convention de Kyoto aux termes de laquelle, entre autres, les applications informatiques mises en oeuvre par les autorités douanières doivent utiliser les normes acceptées à l'échelon international,

SOUHAITANT expressément simplifier et harmoniser les dispositions prises en matière d'interface entre les transporteurs (aériens) et les autorités douanières, notamment en ce qui concerne l'utilisation d'éléments de données, de codes et de syntaxes de messages normalisés,

RECOMMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi qu'aux Unions douanières ou économiques d'adhérer aux normes fixées par la Directive conjointe CCD/IATA relative aux renseignements préalables concernant les voyageurs et à toute future version mise à jour ou révisée de ces normes, aux fins des échanges électroniques de données concernant les voyageurs,

DEMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi qu'aux Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil la date et les modalités de sa mise en application. Le Secrétaire général transmettra ces renseignements aux administrations des douanes des membres du Conseil. Il les transmettra également aux administrations des douanes des membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

x x x

Appendice 13 – Recommandation de l'OMD concernant l'utilisation de l'UNTDED

CONSEIL DE COOPERATION DOUANIERE TC2-3842

RECOMMANDATION DU 26 JUIN 1990*

DU CONSEIL DE COOPERATION DOUANIERE

CONCERNANT L'UTILISATION DU REPERTOIRE

D'ELEMENTS DE DONNEES COMMERCIALES DE L'ONU

(UNTDED)

LE CONSEIL DE COOPERATION DOUANIERE,

SOUHAITANT faciliter l'échange international de données entre les administrations des douanes ainsi qu'entre les administrations des douanes et les intervenants dans le commerce,

CONSIDERANT qu'il est souhaitable d'utiliser dans ces échanges de données commerciales à l'égard des éléments de données des noms, des descriptions et des modes de représentation convenus à l'échelon international et universellement applicables,

CONSIDERANT qu'il est souhaitable que ces noms, ces descriptions et ces modes de représentation soient utilisés pour les éléments de données indépendamment du contexte dans lequel les données commerciales sont échangées (par exemple entre les exportateurs et les transporteurs, les exportateurs et les importateurs, les importateurs et la douane, etc.),

NOTANT que ces éléments de données normalisés peuvent être utilisés avec toutes les méthodes d'échange d'information, sur papier aussi bien que par d'autres moyens de communication, qu'ils peuvent être choisis et transmis un à un ou utilisés dans le cadre d'un système particulier de règles d'échange comme, par exemple, la norme EDIFACT/ONU,

NOTANT EN OUTRE qu'un sous-ensemble de l'UNTDED constitue le Répertoire d'éléments de données EDIFACT (EDED) également recommandé par le Conseil de coopération douanière et expressément conçu pour la télématique,

CONSIDERANT que le Répertoire a été accepté par l'Organisation internationale de normalisation comme norme internationale, sections 1, 2, 3, 4 et 9 du Répertoire constituant la norme internationale ISO 7372,

* Note : La présente Recommandation remplace la Recommandation du Conseil du 21 juin 1988 concernant l'UNTDED.

RECOMMANDE que les Membres du Conseil et tous les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières et économiques utilisent les noms, les descriptions et les modes de représentation des éléments de données figurant dans le Répertoire d'éléments de données commerciales de l'ONU (UNTDED), ainsi que les mises à jour qui seront apportées ultérieurement à ce Répertoire, dans les échanges de données commerciales entre les administrations des douanes ainsi qu'entre les administrations des douanes et les autres intervenants dans le commerce,

INVITE les Membres du Conseil et les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières ou économiques qui acceptent la présente Recommandation à notifier au Secrétaire général leur acceptation, la date à partir de laquelle ils appliqueront la Recommandation et ses conditions d'application. Le Secrétaire général transmettra ces renseignements aux administrations douanières de tous les Membres. Il les transmettra également aux administrations non membres et aux Unions douanières ou économiques qui auront accepté la présente Recommandation.

x
x x

Appendice 14 – Recommandation de l'OMD concernant les règles de syntaxe EDIFACT

CONSEIL DE COOPERATION DOUANIERE

RECOMMANDATION DU 26 JUIN 1990*

DU CONSEIL DE COOPERATION DOUANIERE
CONCERNANT L'UTILISATION DES REGLES DE SYNTAXE

EDIFACT/ONU POUR LES ECHANGES ELECTRONIQUES DE DONNEES

LE CONSEIL DE COOPERATION DOUANIERE,

SOUHAITANT faciliter l'échange international de données entre les administrations des douanes ainsi qu'entre les administrations des douanes et les intervenants dans le commerce,

CONSIDERANT qu'il est souhaitable d'utiliser dans les échanges électroniques de données un ensemble de règles régissant la structure des données qui soit convenu à l'échelon international et universellement applicable,

NOTANT que la Commission économique pour l'Europe des Nations Unies (CEE/ONU) a mis au point un ensemble de normes, de Répertoires et de directives à utiliser dans les échanges électroniques sous le nom d'EDIFACT/ONU (Echange électronique de données pour l'administration, le commerce et les transports) et définis en annexe à la présente Recommandation,

CONSCIENT que les normes, les Répertoires et les directives EDIFACT/ONU peuvent être utilisés indépendamment de leur domaine d'application et que leur usage généralisé dans le commerce international facilitera dans une large mesure l'acheminement des marchandises,

NOTANT que certains éléments des règles EDIFACT/ONU sont par nature des normes auxquelles il convient de se conformer strictement pour que les échanges de données puissent s'opérer avec succès (par exemple les règles de Syntaxe EDIFACT),

NOTANT EN OUTRE que certains autres éléments des règles EDIFACT/ONU sont par nature des directives dont l'application est hautement recommandée (par exemple les directives régissant la conception des messages),

RECOMMANDE que les Membres du Conseil et tous les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières ou économiques appliquent les règles EDIFACT/ONU telles qu'elles sont définies en

* Note : La présente Recommandation remplace la Recommandation du Conseil du 21 juin 1988 concernant les règles de Syntaxe EDIFACT.

annexe à la présente Recommandation, ainsi que les mises à jour qui seront apportées ultérieurement à ces règles, dans l'élaboration des messages électroniques à échanger entre les administrations des douanes et entre les administrations des douanes et les autres intervenants dans le commerce,

INVITE les Membres du Conseil et tous les Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières ou économiques qui acceptent la présente Recommandation à notifier au Secrétaire général leur acceptation, la date à partir de laquelle ils appliqueront la Recommandation et ses conditions d'application. Le Secrétaire général transmettra ces renseignements aux administrations douanières de tous les Membres. Il les transmettra également aux administrations douanières non membres et aux Unions douanières ou économiques qui auront accepté la présente Recommandation.

*
* *

DEFINITION DE L'EDIFACT/ONU

EDIFACT/ONU : Règles de l'ONU régissant l'échange électronique de données pour l'administration, le commerce et les transports. Elles comportent un ensemble de normes, de Répertoires et de directives arrêtés d'un commun accord à l'échelon international et régissant l'échange électronique de données structurées, notamment celles qui ont trait au commerce des biens et services, entre systèmes informatiques indépendants.

Recommandées dans le cadre des Nations Unies, ces règles sont approuvées et publiées par la CE/ONU dans le Répertoire pour l'échange de données commerciales de l'ONU (UNTDED) et sont tenues à jour en application de procédures également convenues d'un commun accord.

L'UNTDED comprend :

- les règles de Syntaxe EDIFACT (ISO 9735)
- les directives régissant la conception des messages
- les directives concernant la mise en oeuvre de la Syntaxe
- le Répertoire d'éléments de données EDIFACT, EDED (sous-ensemble de l'UNTDED)
- la liste de codes EDIFACT, EDCL
- le Répertoire des éléments de données composites EDIFACT, EDCD
- le Répertoire des segments normalisés EDIFACT, EDSD
- le Répertoire des UNSM EDIFACT, EDMD
- les règles de conduite uniformes pour les échanges de données commerciales/télétransmission (UNCID)
- une documentation explicative lorsqu'il y a lieu.

x
x x

Appendice 15 – Recommandation de l'OMD relative à l'utilisation de codes pour les éléments de données

CONSEIL DE COOPERATION DOUANIERE

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'UTILISATION DE CODES POUR LA REPRESENTATION DES ELEMENTS D'INFORMATION

(22 mai 1984)

LE CONSEIL DE COOPERATION DOUANIERE,

DESIREUX de faciliter l'échange de données entre les administrations douanières et entre ces administrations et les intervenants du commerce international,

CONSIDERANT qu'il est souhaitable d'utiliser lors de tels échanges de données, des codes acceptés sur le plan international et universellement applicables pour la représentation des éléments d'information,

EU EGARD aux normes internationales adoptées par l'Organisation internationale de normalisation (ISO) relatives à l'utilisation de codes ou de structures de code pour la représentation des éléments d'information, normes qu'il appuie,

EU EGARD aux Recommandations adoptées par le Groupe de travail sur la facilitation des procédures du commerce international de la Commission économique pour l'Europe (CEE/ONU) qui recommandent que des codes ou des structures de code soient utilisés pour représenter les éléments d'information pour les besoins du commerce international, recommandations qu'il appuie,

CONSIDERANT que les codes ou les structures de code contenus dans les annexes de cette Recommandation constituent une base appropriée pour la représentation des éléments d'information dans les échanges de données,

RECOMMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques, d'utiliser les codes ou les structures de code contenus dans les annexes de la présente Recommandation, ainsi que les versions ultérieures mises à jour ou révisées de ces codes ou de ces structures de code pour la représentation des éléments d'information dans les échanges de données entre les administrations douanières et entre ces administrations et les intervenants du commerce international lorsque la nécessité d'une désignation codée s'impose,

FAIT OBSERVER que l'acceptation de la présente Recommandation implique l'acceptation de ladite Recommandation et d'une au moins des annexes y afférentes et que chaque annexe est considérée comme constituant une Recommandation distincte,

INVITE les Membres du Conseil et les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi que les Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil la date et les modalités de sa mise en application. Le Secrétaire général transmettra ces

renseignements aux administrations des douanes des Membres du Conseil. Il les transmettra également aux administrations des douanes des membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

*
* *

ANNEXE I

Personnes

1. Structure de code recommandée

En ce qui concerne la conception d'un code servant à désigner les personnes (fournisseurs, expéditeurs, exportateurs, destinataires, importateurs et déclarants, etc.), les directives générales relatives à la codification des personnes qui ont été élaborées par le Groupe de travail du CCD chargé de l'étude des applications pratiques des ordinateurs en matière douanière doivent être utilisées.

Ces directives générales, qui ont été élaborées afin d'apporter une assistance pratique aux administrations des douanes à l'échelon national et qui sont compatibles avec la norme internationale ISO 6523 (échange de données, structure pour l'identification des organisations) figurent dans le dossier sur l'informatisation des opérations douanières.

2. Description sommaire

Les directives générales visent à uniformiser la codification des personnes physiques et morales participant aux opérations du commerce international et intéressant la douane (par exemple, les importateurs, les exportateurs, les agents en douane, etc.). Elles ont trait en particulier à la fonction des codes, aux personnes identifiées, au choix des codes, à la longueur et au format des codes, à l'identification des autres éléments, à l'identification des fournisseurs étrangers, à l'utilisation de caractères de contrôle et aux critères et aux considérations se rapportant aux systèmes à prendre en compte dans l'élaboration des codes.

Comme indiqué ci-dessus, les directives sont compatibles avec la norme internationale ISO 6523 qui préconise la structure ci-après pour l'identification des organisations aux fins des échanges de données : a) désignation codée internationale (code de longueur fixe à quatre chiffres); b) code de l'organisation et c) nom de l'organisation. Le code d'organisation composé de 14 caractères au maximum qui permet d'identifier séparément une organisation dans un système de codification des organisations. Le code d'organisation peut impliquer l'utilisation de caractères alphabétiques, numériques ou alphanumériques et il est recommandé que le code comporte un caractère de contrôle pouvant être incorporé dans le code d'organisation ou figurer dans une zone distincte.

ANNEXE II

Marques d'identification des conteneurs

1. Codes recommandés

L'attention est appelée sur le code qui figure dans la norme internationale 6346 (conteneurs pour le transport de marchandises -codage, identification et marquage) et qui est destiné à la représentation des données relatives aux conteneurs pour le transport de marchandises utilisés dans les modes de transport autres que le transport aérien, ainsi que sur le code mis au point par l'IATA pour la représentation des données relatives aux conteneurs utilisés pour le fret aérien.

Lorsque les données relatives à l'identification des conteneurs sont saisies et exploitées par la douane, il est recommandé de prévoir 17 caractères dans les programmes d'ordinateur et les documents qui leur sont associés, de façon à pouvoir employer le code ISO (éventuellement 17 caractères au total), ainsi que les versions actuelles et futures du code de l'IATA (9 et 12 caractères respectivement).

2. Description sommaire

A. Code ISO

La norme internationale 6346 établit un système de marquage des conteneurs permettant de fournir à l'aide d'un code alphanumérique à 17 caractères : une identification internationale unique, comprenant un code de propriétaire, un numéro de série et un code de pays; un système de vérification de l'exactitude des données relatives au code de propriétaire et au numéro de série; et des renseignements sur les caractéristiques dimensionnelles et sur le type du conteneur.

B. Code de l'IATA

Le code mis au point par l'IATA pour la représentation des éléments d'information relatifs aux conteneurs utilisés pour le fret aérien comprend actuellement 9 caractères alpha-numériques (type de conteneur, dimensions et compatibilité, numéro de série et code de propriétaire). En 1990, le code de l'IATA comprendra 12 caractères alphanumériques dont un chiffre d'autocontrôle.

ANNEXE III

Dates

1. Code recommandé

La représentation fournie dans la Recommandation n° 7 de la CEE/ONU (représentation numérique des dates, heures et intervalles de temps) qui est fondée notamment sur les normes internationales 2014 (représentation entièrement numérique des dates du calendrier) et 3307 (échange d'information - représentation de l'heure) doit être utilisée pour la représentation des dates et des heures (date et heure de départ, date et heure d'arrivée, date du contrat, date de l'opération de change, date de l'acceptation de la déclaration, date du dédouanement des marchandises, etc.).

2. Description sommaire

La Recommandation n° 7 de la CEE/ONU (représentation numérique des dates, heures et intervalles de temps) repose notamment sur les normes internationales ISO 2014 et 3307.

La norme ISO 2014 prévoit un mode de représentation entièrement numérique des dates du calendrier grégorien déterminées par les éléments : année, mois et jour. Elle recommande que toutes les dates sous forme entièrement numérique soient placées dans l'ordre suivant : année - mois -jour (à savoir, AAAAMMJJ) et soient constituées de quatre, deux et deux chiffres représentant l'année, le mois et le jour, respectivement.

La norme ISO 3307 vise à établir une représentation uniforme du temps reposant sur le système du temps solaire moyen. Elle fournit un mode de représentation de l'heure locale sous forme numérique pour l'échange d'information dans les systèmes de données. L'heure locale est définie comme l'heure légale au point d'origine. Dans le système du temps solaire moyen, l'heure locale peut être exprimée par la combinaison des éléments heures, minutes et secondes, par exemple, heures et minutes (HHMM).

En ce qui concerne la date, l'attention est appelée sur le fait que la Recommandation n° 7 de la CEE/ONU prévoit l'utilisation de deux caractères seulement pour représenter l'année (AAMMJJ, par exemple).

ANNEXE IV

Monnaies

1. Code recommandé

Le code alphabétique de l'ISO à trois lettres pour la représentation des monnaies qui figure dans la norme internationale 4217 (code pour la représentation des monnaies et types de fonds) doit être utilisé pour la représentation des monnaies.

2. Description sommaire

La norme ISO 4217 prévoit un code alphabétique à trois lettres et un code numérique à trois chiffres équivalent pour la représentation des monnaies et des types de fonds.

Les deux premiers caractères du code alphabétique de la norme ISO 4217 constituent un code d'identification unique de l'autorité monétaire à laquelle il est attribué. Ce code est dérivé, autant que possible, du code des pays alpha-2, de l'ISO qui figure dans la norme ISO 3166 (code pour la représentation des noms de pays) et qui est recommandé par le Conseil de coopération douanière et par le Groupe de travail sur la facilitation des procédures du commerce international de la Commission économique pour l'Europe (CEE/ONU). Le troisième caractère du code alphabétique est un indicateur, mnémonique de préférence, dérivé du nom de l'unité monétaire principale ou du nom du type de fonds. Dans les applications non bancaires, les deux premiers caractères du code suffisent à identifier la monnaie. Le code numérique est dérivé, dans la mesure du possible, du "United Nations Standard Country or Area Code".

La Recommandation n° 9 adoptée en février 1978 par le Groupe de travail sur la facilitation des procédures du commerce international de la CEE/ONU prévoit l'utilisation du code à trois lettres de l'ISO pour la représentation des monnaies aux fins du commerce international.

ANNEXE V

Codes de pays

1. Codes recommandés

Les codes alpha-2 de représentation des pays préconisés par la norme internationale ISO 3166 et mentionnés dans la recommandation n° 3 de la CEE/ONU, doivent être utilisés pour la représentation des noms de pays dans les échanges internationaux.

Toutefois, il est à noter que l'acceptation de la présente Recommandation de l'OMD n'exclut pas l'emploi d'autres codes mentionnés dans la norme ISO 3166 pour représenter les noms de pays en vue de certaines applications (par exemple, le code ISO alpha-3 de pays pour les passeports lisibles à la machine, comme prévu dans les Directives CCD/IATA sur les renseignements préalables concernant les voyageurs). L'acceptation de la présente Recommandation ne fait pas non plus obstacle à l'utilisation de codes autres que ceux de l'ISO à des fins nationales, ou internationales lorsqu'il s'agit de pays appartenant à une Union douanière ou économique.

2. Description sommaire

Le code ISO alpha-2 des pays est un code à deux lettres.

ANNEXE VI

Désignation des marchandises

et positions tarifaires ou statistiques

1. Structure de code recommandée

Le Système harmonisé de désignation et de codification des marchandises doit être utilisé.

2. Description sommaire

Le Système harmonisé de désignation et de codification des marchandises est une nomenclature polyvalente à six chiffres pour les produits transportables qui répond simultanément aux besoins des autorités douanières, des spécialistes des statistiques du commerce extérieur ou de la production, des transporteurs et des producteurs. Ce système se prête au traitement automatique et à la transmission des données et permet de disposer d'une terminologie et d'un code communs pour spécialiser expressément 5019 catégories de produits recensés sous une forme plus détaillée à partir de 1241 positions à quatre chiffres. Ces positions à quatre chiffres sont le résultat d'une révision et d'une mise à jour approfondies non seulement de chaque position mais aussi de la structure même de la Nomenclature du Conseil de coopération douanière (NCCD). Le Système harmonisé peut être, le cas échéant, subdivisé encore davantage pour répondre aux impératifs qui se manifestent le cas échéant sur le plan national et international.

ANNEXE VII

Régimes douaniers

1. Code recommandé

Les directives générales et le code à un chiffre élaborés par le Groupe de travail du CCD chargé de l'étude des applications pratiques des ordinateurs en matière douanière doivent être utilisés pour la représentation des régimes douaniers. Les directives générales et le code à un chiffre figurent dans le dossier sur l'informatisation des opérations douanières.

2. Description sommaire

Le code élaboré par le Groupe de travail du CCD chargé de l'étude des applications pratiques des ordinateurs en matière douanière pour la représentation des régimes douaniers est un code très général à un chiffre dans le cadre duquel les principaux régimes douaniers sont identifiés et qui permet aux utilisateurs d'élaborer des codes uniques répondant à des besoins nationaux ou internationaux.

ANNEXE VIII

Unités de mesure

1. Codes recommandés

Les codes figurant dans la Recommandation de la CEE/ONU n° 20 (codes désignant les unités de mesure utilisées dans le commerce international) sont à utiliser pour la représentation des unités de mesure.

2. Description sommaire

Les codes d'unités de mesure mis au point par la CEE/ONU comportent un code alphabétique à trois lettres de longueur fixe et un code numérique à trois chiffres de longueur fixe.

ANNEXE IX

Code mode de transport

1. Codes recommandés

Les codes contenus dans la Recommandation n° 19 de la CEE/ONU (Codes pour représenter les modes de transport et moyens de transport correspondants utilisés pour le commerce international) doivent être utilisés pour la représentation des modes de transport.

2. Description sommaire

Les codes modes de transport mis au point par la CEE/ONU sont constitués par un code numérique à un chiffre. Toutefois, il est possible d'utiliser un deuxième chiffre lorsque le code de base doit être subdivisé.

*
* *

Appendice 16 – Recommandation de l'OMD concernant les renseignements douaniers traités par ordinateur

ORGANISATION MONDIALE DES DOUANES*

RECOMMANDATION DE L'ORGANISATION MONDIALE DES DOUANES CONCERNANT LA TRANSMISSION ET L'AUTHENTIFICATION PAR VOIE ELECTRONIQUE DES RENSEIGNEMENTS DOUANIERS ET AUTRES RENSEIGNEMENTS EXIGES
(16 juin 1981 révisée 24 juin 2005)

L'ORGANISATION MONDIALE DES DOUANES,

SOUCIEUSE d'étendre les possibilités d'utilisation des systèmes informatiques de la douane et des usagers du commerce international en permettant aux déclarants de transmettre à la douane les renseignements douaniers par des moyens électroniques ou d'autres moyens automatiques,

CONSIDERANT que le traitement automatique des données, le commerce électronique, notamment la télématique et les techniques garantissant la sécurité permettent de transmettre, de valider et d'authentifier autrement que par des documents sur papier et une signature manuscrite les renseignements exigés par la douane et traités par ordinateur (données figurant dans les déclarations de marchandises, les manifestes, les licences, etc., par exemple); que parmi les méthodes pouvant être utilisées on peut citer l'emploi des mots de passe uniques propres au déclarant et transmis avec les renseignements, les clés de logiciel pour encoder les données et produire des signatures électroniques; que conformément aux dispositions de la législation nationale ou suite à un engagement souscrit par le déclarant, l'utilisation pour la transmission des renseignements douaniers de ces techniques propres à garantir la sécurité peut être considérée comme engageant sa responsabilité personnelle au même titre que s'il avait apposé sa signature sur un document sur papier,

TENANT COMPTE de la "Recommandation sur l'authentification des documents commerciaux par des moyens autres que la signature" qui a également été adoptée, en mars 1979, par le Groupe de travail précité et qui fait notamment observer que l'adoption généralisée des méthodes mécaniques ou électroniques de transmission des données appelle la modification des législations nationales et des conventions internationales en vigueur et de la pratique commerciale actuelle en matière de signature,

ET TENANT EGALEMENT COMPTE de la ''Loi type sur le commerce électronique'' de la Commission des Nations Unies pour le droit commercial international (CNUDCI) adoptée par les Nations Unies en décembre 1996 et de la ''Loi type sur les signatures électroniques'' de la CNUDCI adoptée par les Nations Unies en décembre 2001 en tant

* Créée en 1952 sous le nom de Conseil de coopération douanière (CCD).

que références utiles pour élaborer une législation nationale sur le commerce électronique et les signatures numériques,

RECOMMANDE aux Etats membres du Conseil, ainsi qu'aux membres de l'Organisation des Nations Unies ou à ses institutions spécialisées et aux Unions douanières et économiques :

1. D'offrir au déclarant, aux conditions fixées par les autorités douanières, la possibilité d'utiliser différents supports électroniques (notamment réseaux valeur ajoutée, Internet, réseaux sans fil, disquettes, bandes, etc.) pour transmettre à la douane à des fins de traitement automatique les renseignements qu'elle exige et pour qu'elle y donne automatiquement suite.

2. D'accepter de la part des déclarants et des administrations publiques, aux conditions fixées par les autorités douanières, les renseignements exigés par la douane qui sont transmis sur des supports électroniques, validés et authentifiés par des moyens garantissant la sécurité sans qu'il soit nécessaire de déposer des documents sur papier munis d'une signature manuscrite.
3. De faire en sorte, lorsque les gouvernements n'ont pas mis en place de ''guichet unique'' électronique permettant aux déclarants de présenter en une seule fois et à un point d'accès unique, les renseignements exigés aux fins des transactions transfrontalières internationales, que les prescriptions et les spécifications techniques relatives à l'authentification des renseignements exigés échangés par voie électronique soient coordonnées entre l'ensemble des services publics intéressés.

4. D'accepter, lorsque la loi n'autorise pas encore la transmission par des moyens électroniques des renseignements exigés par la douane, que celle-ci autorise les déclarants, dans les conditions à définir par la douane ou par d'autres autorités compétentes, à présenter sur papier ordinaire les renseignements exigés par la douane.

5. D'accepter, lorsque la télématique, les techniques garantissant la sécurité et l'informatique sont utilisées mais qu'en raison de restrictions d'ordre juridique il y a toujours lieu de présenter des documents sur papier et des signatures manuscrites, le dépôt périodique de ces documents ou leur conservation dans les locaux du déclarant, conformément aux conditions arrêtées par la douane.

DEMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil la date et les modalités de sa mise en applications. Le Secrétaire général transmettra ces renseignements aux administrations des douanes des Membres du Conseil. Il les transmettra également aux administrations des douanes des membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

x x x

Appendice 17 – Recommandation de l'OMD concernant l'utilisation des normes CCD/IATA

CONSEIL DE COOPERATION DOUANIERE

**RECOMMANDATION DU 21 JUIN 1988
DU CONSEIL DE COOPERATION DOUANIERE**

CONCERNANT L'UTILISATION DES NORMES CCD/IATA

REGISSANT LES ECHANGES DE DONNEES

LE CONSEIL DE COOPERATION DOUANIERE,

VU le haut degré d'automatisation des compagnies aériennes et le nombre croissant d'administrations des douanes qui s'informatisent,

VU la multiplication des échanges électroniques de données dans le commerce mondial et les avantages que présentent les transactions commerciales sans support papier,

CONSCIENT que la mise en place d'interfaces entre les systèmes automatisés des compagnies aériennes et des administrations des douanes peut faciliter les échanges électroniques de données et réduire le volume des écritures,

CONSTATANT que l'automatisation du traitement des données concernant le fret accélère le dédouanement des envois aériens et présente des avantages importants pour le contrôle douanier,

COMPTE TENU de l'Annexe J.1. de la Convention internationale du 18 mai 1973 pour la simplification et l'harmonisation des régimes douaniers qui dispose notamment que les autorités douanières doivent utiliser des normes acceptées à l'échelon international pour la mise en oeuvre de leurs applications informatiques,

SOUHAITANT expressément simplifier et harmoniser les dispositions régissant les interfaces entre les compagnies aériennes et les autorités douanières, notamment en ce qui concerne l'utilisation d'éléments d'information normalisés, les codes et la syntaxe des messages,

RECOMMANDE aux Membres du Conseil et aux membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques, d'utiliser les normes énoncées dans le manuel qui répertorie les normes CCD/IATA régissant les échanges de données ainsi que les versions ultérieures mises à jour ou révisées pour la mise en place d'interfaces entre les systèmes automatisés de la douane et les compagnies aériennes,

INVITE les Membres du Conseil et les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi que les Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil la date et les modalités de sa mise en application. Le Secrétaire général transmettra ces

renseignements aux administrations des douanes des Membres du Conseil. Il les transmettra également aux administrations des douanes des membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques ayant accepté la présente Recommandation.

Appendice 18- RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'UTILISATION DU MODELE DE DONNEES DE L'OMD

CONSEIL DE COOPERATION DOUANIERE

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE RELATIVE A L'UTILISATION DU MODELE DE DONNEES DE L'OMD

(27 juin 2009)

LE CONSEIL DE COOPERATION DOUANIERE,

SOUHAITANT faciliter les échanges internationaux de données entre administrations des douanes ainsi qu'entre les administrations des douanes et les autorités chargées du contrôle des frontières, les intervenants dans le commerce et les autres parties impliquées dans les transactions internationales et dans les mouvements transfrontaliers de marchandises,

CONSIDERANT qu'il est souhaitable de recourir à des normes internationales lors de la définition d'éléments de données et de l'élaboration des messages électroniques à utiliser pour ces transactions internationales,

CONSIDERANT que le Modèle de données de l'OMD

(i) représente le jeu maximal de données exigées aux fins des informations nécessaires avant l'arrivée et le départ, ainsi que de la mainlevée et du dédouanement aux frontières des marchandises et des moyens de transport à l'importation, à l'exportation et en transit.
(ii) a été élaboré à l'aide d'un jeu harmonisé de données exigées par des administrations des douanes Membres et plusieurs autorités chargées du contrôle aux frontières, et
(iii) s'appuie sur des normes internationales largement adoptées et reconnues.

RECOMMANDE que, dans la mesure du possible, les Membres du Conseil et tous les membres de l'Organisation des Nations Unies ou de ses institutions spécialisées ainsi que les Unions douanières et économiques :

1. adoptent le Modèle de données de l'OMD pour identifier et définir toutes les données officielles exigées aux frontières dans le cadre des formalités préalables à l'arrivée et au départ et des procédures à l'importation, à l'exportation et en transit.
2. utilisent les éléments de données de l'OMD, leurs noms et leurs numéros de référence (ID de l'OMD), leurs descriptions et les modes de représentation de leurs caractères (y compris les listes de codes suggérées) pour décrire et composer les messages électroniques.
3. utilisent les messages électroniques normalisés décrits dans le Modèle de données de l'OMD pour les messages électroniques entre les gouvernements ainsi qu'entre les gouvernements et les entreprises.

DEMANDE aux Membres du Conseil et à tout Membre de l'Organisation des Nations Uniesou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire Général leur acceptation, la date à partir de laquelle ils appliqueront la Recommandation et ses conditions d'application. Le Secrétaire

général transmettra ces renseignements aux administrations douanières de tous les Membres. Il les transmettra également aux administrations non membres et aux Unions douanières ou économiques qui auront accepté la présente Recommandation.

*

* *

Appendice 19 RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE[1] RELATIVE A L'EMPLOI DES RENSEIGNEMENTS PREALABLES CONCERNANT LES VOYAGEURS (RPCV) ET DES DOSSIERS PASSAGERS (PNR) AFIN D'ASSURER L'EFFICACITE DES CONTROLES DOUANIERS

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE[2] RELATIVE A L'EMPLOI DES RENSEIGNEMENTS PREALABLES CONCERNANT LES VOYAGEURS (RPCV) ET DES DOSSIERS PASSAGERS (PNR) AFIN D'ASSURER L'EFFICACITE DES CONTROLES DOUANIERS

(juin 2012)

LE CONSEIL DE COOPERATION DOUANIERE,

PRENANT ACTE de la menace croissante que ne cessent de soulever les formes graves de la criminalité transnationale, et notamment le trafic illicite de drogue et d'autres marchandises de contrebande, qui est très préoccupante pour le bien-être social, la sécurité et la prospérité des nations du monde entier,

PRENANT ACTE de la croissance continue du volume des voyages transfrontaliers et des enjeux qui en résultent s'agissant de faciliter la circulation des voyageurs en règle,

EU EGARD aux dispositions de la Convention de Kyoto révisée[3] et, notamment, de celles du Chapitre 6 de l'Annexe générale sur les contrôles douaniers et du Chapitre 1 de l'Annexe spécifique J sur les voyageurs,

RECONNAISSANT que les administrations des douanes exercent la responsabilité première du contrôle des mouvements transfrontières de marchandises, de moyens de transport et de personnes, et qu'elles sont donc idéalement placées pour prévenir, détecter et réprimer le trafic illicite de drogue et d'autres marchandises de contrebande aux frontières avant que celles-ci ne se dispersent sur le territoire des différents pays,

PRENANT ACTE des incidents qui témoignent de l'existence d'un lien étroit entre les formes graves de la criminalité transnationale et le terrorisme, et de la nécessité de diminuer les risques perçus que soulèvent les voyageurs,

---

1 Conseil de coopération douanière est la dénomination officielle de l'Organisation mondiale des douanes (OMD).

2 Conseil de coopération douanière est la dénomination officielle de l'Organisation mondiale des douanes (OMD).

3 Convention internationale relative à la simplification et à l'harmonisation des régimes douaniers (amendée).

RECONNAISSANT que le meilleur moyen de parvenir à un équilibre approprié entre les besoins en matière de lutte contre la fraude douanière et la facilitation des voyages licites consiste à lutter contre la fraude douanière en se fondant sur le renseignement, et que l'emploi des RPCV et/ou des PNR pour évaluer les risques aiderait considérablement les administrations des douanes à concevoir et à exploiter le renseignement le plus utilement possible aux fins du contrôle des voyageurs,

SOUHAITANT harmoniser les arrangements conclus en matière d'interface entre les administrations des douanes et les entreprises, notamment en ce qui concerne la transmission électronique des données des RPCV et/ou des PNR conformément aux formats de messages et aux éléments de données normalisés à l'échelon international,

ESTIMANT que le contrôle efficace des formes graves de la criminalité transnationale, et notamment du trafic illicite de drogue et d'autres marchandises de contrebande, aux frontières peut être largement facilité par la coopération entre les administrations des douanes et d'autres services compétents en matière de contrôle aux frontières à l'échelon national et international, et que les échanges d'informations peuvent apporter une aide significative en matière d'évaluation des risques et de ciblage et, par conséquent, améliorer la facilitation des voyages à caractère licite,

RECOMMANDE aux Membres du Conseil et aux Unions douanières ou économiques :

1. de veiller à ce que la prévention, la détection et la répression des formats graves de la criminalité transnationale, et notamment du trafic illicite de drogue et d'autres marchandises de contrebande, soient préconisées et demeurent l'une des priorités des programmes et de la stratégie de lutte contre la fraude des autorités douanières,

2. de s'efforcer d'obtenir la coopération la plus entière possible des compagnies aériennes et autres sociétés internationales de transport de voyageurs pour aider la douane à s'acquitter de sa mission,

3. d'utiliser les renseignements préalables, à savoir, les RPCV et/ou les PNR, pour évaluer les risques liés aux voyageurs et :

    - d'établir des prérogatives légales permettant d'obtenir l'accès aux données des RPCV et/ou des PNR, ou d'en exiger le transfert, l'emploi et le stockage, conformément aux modalités fixées et à la portée des données exigées à cette fin, et de mettre en place des mécanismes de protection des données pertinentes,

    - de respecter les normes, les formats et les procédures techniques fixés dans les directives reconnues à l'échelon international, et

    - dans toute la mesure possible, de participer aux travaux de conception ou de mise à jour des normes, des procédures et des formats techniques internationaux, ainsi que des meilleures pratiques relatives à leur application,

4. de promouvoir la coopération avec les autres administrations des douanes et de leur apporter un soutien, dans le contexte du cadre juridique national, y compris l'échange de renseignement et d'expérience dans l'emploi des RPCV et/ou des PNR aux fins de l'identification plus efficace des voyageurs potentiellement à haut risque.

INVITE les Membres du Conseil et les Unions douanières ou économiques qui acceptent la présente Recommandation à notifier au Secrétaire général du Conseil la date à compter de laquelle ils appliqueront ladite Recommandation et les modalités de sa mise en application.

Appendice 20 : RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE[4] RELATIVE A LA DEMATERIALISATION DES DOCUMENTS JUSTIFICATIFS

RECOMMANDATION DU CONSEIL DE COOPERATION DOUANIERE5 RELATIVE A LA DEMATERIALISATION DES DOCUMENTS JUSTIFICATIFS

(Juin 2012)

LE CONSEIL DE COOPERATION DOUANIERE,

PRENANT ACTE que les administrations des douanes ont pour une large part mis en place des systèmes automatisés de dédouanement du fret et se sont engagées à appliquer la technologie de l'information à l'appui des opérations douanières, lorsque cela est rentable et efficace pour la douane et pour les entreprises,

CONSIDERANT que l'utilisation des documents sur support papier en commerce international est coûteuse, longue et propice aux erreurs et aux irrégularités,

EU EGARD aux dispositions du Chapitre 3 de l'Annexe générale de la Convention de Kyoto révisée[6] concernant la présentation électronique des documents justificatifs à la douane,

RECONNAISSANT la conception rapide de solutions rentables, sûres et fiables pour les systèmes de gestion et de conservation des documents électroniques, et l'adoption généralisée de ces solutions par les milieux commerciaux et les administrations,

RECONNAISSANT que les organisations internationales, les services publics et les associations professionnelles mettent de plus en plus souvent en place des formats normalisés pour les documents électroniques tels que licences, certificats et permis, et favorisent leur utilisation tout au long des transactions commerciales internationales,

VISANT à promouvoir les transactions dématérialisées aux fins du dédouanement en tant que variante aux exigences documentaires sur papier,

SOUHAITANT réduire les coûts pour les entreprises et simplifier les procédures commerciales en allégeant la charge que représentent la remise, le stockage et la présentation des documents justificatifs originaux sur support papier au cours des procédures douanières,

et

SOUHAITANT améliorer le contrôle douanier en recourant efficacement aux vérifications automatisées et en adoptant le principe de la gestion des risques,

---

[4] Conseil de coopération douanière est la dénomination officielle de l'Organisation mondiale des douanes (OMD).

[5] Conseil de coopération douanière est la dénomination officielle de l'Organisation mondiale des douanes (OMD).

[6] Convention internationale relative à la simplification et à l'harmonisation des régimes douaniers (amendée).

RECOMMANDE aux Membres du Conseil et à tous les Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, ainsi qu'aux Unions douanières ou économiques, dans la mesure du possible :

(1) d'identifier les documents justificatifs qui doivent normalement accompagner les déclarations de chargement et de marchandises et de déterminer la nécessité de présenter ces documents aux fins du dédouanement afin de les éliminer;
(2) de supprimer l'obligation de présenter les documents justificatifs sur support papier s'ils ont déjà été présentés sous format électronique;
(3) de procéder à la mainlevée et au dédouanement du fret sur la seule base d'une déclaration électronique et d'une vérification automatisée;
(4) de faire en sorte que les systèmes automatisés de dédouanement puissent vérifier automatiquement les informations contenues dans les documents justificatifs dématérialisés lorsque ces informations sont accessibles par voie électronique :
   a) dans les bases de données des autres services publics;
   b) dans les environnements de guichet unique (et les systèmes communautaires de fret);
   c) dans les répertoires privés.

INVITE les Membres du Conseil, les Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, et les Unions douanières ou économiques qui acceptent la présente Recommandation de notifier au Secrétaire général du Conseil la date à compter de laquelle ils appliqueront ladite Recommandation et les modalités de son application. Le Secrétaire général transmettra ces renseignements aux administrations douanières de tous les Membres du Conseil. Il les transmettra également aux administrations douanières des Membres de l'Organisation des Nations Unies ou de ses institutions spécialisées, et aux Unions douanières ou économiques qui ont accepté la présente Recommandation.

x

x x