ORGANISATION HYDROGRAPHIQUE INTERNATIONALE

DISPOSITIF DE PROTECTION DES DONNEES DE L'OHI

Edition 1.1.1 – Avril 2012

Publication S-63 de l'OHI

Publiée par le
Bureau hydrographique International
MONACO

Avis de droit d'auteur

ORGANISATION HYDROGRAPHIQUE INTERNATIONALE

DISPOSITIF DE PROTECTION DES DONNEES DE L'OHI

Edition 1.1.1 – Avril 2012

Publication S-63 de l'OHI

Publiée par le
Bureau hydrographique international
4, Quai Antoine 1er
B.P 445 - MC 98011 MONACO Cedex
Principauté de Monaco
Tél: +(377) 93 10 81 00
Téléfax: +(377) 93 10 81 40
Courriel: info@iho.int
Web: www.iho.int

Page laissée en blanc intentionnellement

PREFACE

La violation du droit d'auteur et le piratage des données sont des problèmes omniprésents de l'ère numérique. Les cartes électroniques de navigation (ENC) n'en sont pas exemptées. En plus de l'impact économique, la distribution non-officielle des informations nautiques a des répercussions importantes en matière de sécurité. En conséquence, les distributeurs officiels d'informations nautiques ont cherché à protéger leurs données et à fournir au navigateur un certificat d'authenticité grâce à l'adoption d'un dispositif de sécurité.

En Septembre 2000, il a été demandé aux Etats membres de l'OHI leur point de vue sur le développement d'un dispositif de sécurité recommandé (RSS) (voir: Lettre circulaire du BHI 38/2000). Une large majorité des Etats membres a répondu qu'ils souhaitaient avoir leurs données chiffrées et qu'ils approuvaient l'adoption par l'OHI d'un RSS unique (voir lettre circulaire du BHI 15/2001 Rev.1). La majorité des Etats membres ayant répondu était en faveur de l'adoption du dispositif de sécurité Primar en tant que RSS de l'OHI, étant entendu qu'il représentait à l'époque la norme de facto en ce qui concerne la protection ENC et que la majorité des fabricants d'ECDIS a déjà développé au sein de leurs systèmes les facilités de déchiffrement nécessaires

Le Comité de l'OHI sur les besoins hydrographiques pour les systèmes d'information (CHRIS, aujourd'hui HSSC : Hydrographic Services and Standards Committee), à sa 13ème réunion, (Athènes, Grèce, Septembre 2001), a reconsidéré la question du RSS et a convenu qu'un petit groupe consultatif étudierait les implications qu'il y aurait pour le BHI à devenir Administrateur du dispositif de sécurité dans le cadre d'un RSS et à assumer la responsabilité de la mise à jour d'un RSS.

Le Groupe de travail sur le dispositif de la protection des données (DPSWG) a signalé au BHI en janvier 2002 qu'il n'y avait aucune implication technique pour le BHI à devenir Administrateur du dispositif de sécurité et que le niveau de travail nécessaire pour administrer le dispositif de sécurité rentrerait dans les limites des ressources du BHI. Le DPSWG a, en outre, fourni un plan de développement d'une Version 1 du RSS de l'OHI, basée sur le dispositif de sécurité Primar. Ce rapport a été approuvé par les membres du CHRIS en février 2002 et le DPSWG a été chargé de mettre au point la Version 1 du RSS de l'OHI.

Les résultats ont été présentés au CHRIS, à sa 14e réunion (Shanghai, Chine, août 2002), laquelle a recommandé que le dispositif de sécurité ENC, tel que mis au point par le DPSWG, soit présenté aux Etats membres de l'OHI pour adoption en tant que Version 1 d'un RSS de l'OHI et que le rôle d'Administrateur du dispositif de sécurité soit transféré au BHI. Ces propositions (voir LC du BHI 44/2002) ont été approuvées par une majorité des Etats membres (voir LC du BHI 66/2002). En conséquence, l'Edition 1.0 du dispositif de protection des données de l'OHI a été adoptée en octobre 2003, en tant que Publication S-63.

La 18e réunion du CHRIS (Cairns, Australie, Septembre 2006) a chargé le DPSWG de développer une édition révisée de la S-63 avec les indications suivantes :

- Aucun nouvel élément ne serait introduit; les changements seraient maintenus au minimum.
- Les indications relatives à la S-63 publiées seraient incluses dans la norme.
- La S-63 serait réorganisée de manière à regrouper les sujets concernant le BHI, administrateur du dispositif, ceux sur les fournisseurs de données et ceux sur les fabricants d'ECDIS, respectivement.
- La mise en œuvre correcte de la norme de l'OHI serait décrite de façon plus précise.

En conséquence, un projet d'Edition 1.1 de la S-63 fut préparé par le DPSWG et approuvé par le CHRIS à sa 19e réunion (Rotterdam, Pays-Bas, novembre 2007). Il fut par la suite approuvé par les Etats membres et adopté en mars 2008. L'édition 1.1 incluait une documentation, des données d'essai et une méthode de fourniture d'ENC au moyen d'un « média de grande capacité ».

En avril 2012, des changements mineurs ont été apportés à l'édition 1.1 pour s'affranchir de la limitation hexadécimale du M_ID et accroître le nombre des valeurs possibles de M_ID que le dispositif peut gérer. Il en a résulté cette édition 1.1.1 de la S-63 qui remplace l'édition 1.1. Les changements à cette norme, ainsi que tout développement ultérieur, continueront d'être coordonnés par le DPSWG sous la direction du HSSC.

Page laissée en blanc intentionnellement

TABLE DES MATIERES

GLOSSAIRE 1

1 INTRODUCTION 3

1.1 DESCRIPTION GENERALE 3
1.2 PARTICIPANTS AU DISPOSITIF 4
1.2.1 Administrateur du dispositif 4
1.2.2 Fournisseurs de données 4
1.2.3 Clients utilisateurs de données 4
1.2.4 Fabricants (OEM) 4
1.2.5 Relations des participants à la S-23 5
1.3 REFERENCES 5
1.4 COMPATIBILITE AVEC LES VERSIONS PRECEDENTES 6
1.5 STRUCTURE DU DOCUMENT 6
1.6 MISE A JOUR 7
1.7 SOUTIEN 7

2 COMPRESSION DES DONNEES 9

2.1 VUE D'ENEMBLE 9
2.2 ALGORITHME DE COMPRESSION 9
2.3 FICHIERS COMPRESSES 9

3 CHIFFREMENT DES DONNEES 11

3.1 QUELLES DONNEES SONT CHIFFREES? 11
3.2 DE QUELLE MANIERE SONT-ELLES CHIFFREES? 11
3.2.1 Chiffrement des informations relatives aux ENC 11
3.2.2 Chiffrement des autres informations relatives au dispositif de protection 11
3.2.3 Algorithme de chiffrement – Blowfish 11

4 AUTORISATION D'EXPLOITATION DES DONNEES 13

4.1 INTRODUCTION 13
4.2 LE PERMIS D'UTILISATEUR 13
4.2.1 Définition du permis d'utilisateur 14
4.2.2 Format HW_ID 14
4.2.3 Format du total de contrôle 14
4.2.4 Format M_ID 15
4.2.5 Format M_KEY 15
4.3 LE PERMIS DE CELLULE 15
4.3.1 Le fichier de permis (PERMIT.TXT) 16
4.3.2 Le fichier de permis – Formats des en-tête 16
4.3.3 Champ d'enregistrement de permis 17
4.3.4 Définition du permis de cellule 18
4.3.5 Format du permis de cellule 18
4.3.6 Fichier additionnel (en option) 19

5 AUTHENTICATION DES DONNEES 21

5.1 INTRODUCTION AU CONTROLE DE L'AUTHENTIFICATION ET DE L'INTEGRITE DES DONNEES 21
5.1.1 Vérification de l'Administrateur du dispositif 23
5.1.2 Intégrité des données 23
5.2 CERTIFICATS NUMERIQUES (AUTHENTIFICATION DE L'ADMINISTRATEUR DU DISPOSITIF) 23
5.2.1 La clé publique de l'Administrateur du dispositif 24
5.2.2 Nouveaux fournisseurs de données 24
5.3 SIGNATURES NUMERIQUES (VERIFIE L'INTEGRITE DES DONNEES) 24
5.3.1 Vue d'ensemble technique des signatures numériques 25
5.3.2 Convention de dénomination du fichier de signature ENC 25
5.3.3 Archivage du fichier de signature ENC 26

5.4 FORMATS DU FICHIER D'AUTHENTIFICATION DES DONNEES 26
5.4.1 Eléments du fichier 26
5.4.1.1 En tête des éléments et(formattage de la chaîne des données 26
5.4.2 Exémples de formats de fichier, de certificat et de signature 27
5.4.2.1 Format PQG 27
5.4.2.2 Le format X (Clé privée) 27
5.4.2.3 Le format Y (OHI ou clé publique de fournisseur de données) 28
5.4.2.4 Le format de certificat numérique de l'Administrateur du dispositif (X509v3) 28
5.4.2.5 Le format de clé auto-signée (SSK) 28
5.4.2.6 Le format de fichier de certificat de signature numérique signé par L'Administrateur du dispositif 29
5.4.2.7 Le format de fichier de signature ENC 29

6 GESTION DES DONNEES 29

6.1 INTRODUCTION 31
6.2 LISTAGE DE PRODUIT ENC (PRODUCTS.TXT) 32
6.2.1 Structure du fichier de la liste de produit 33
6.2.2 En-tête de la liste de produit 33
6.2.3 Section 'ENC' de la liste de produit 33
6.2.3.1 Gestion des cellules annulées (Fournisseurs de données) 36
6.2.3.2 Gestion des cellules annulées (Clients utilisateurs de données) 36
6.2.3.3 Remplacements des cellules ENC annulées 36
6.2.4 Section 'ECS' de la liste de produit 37
6.3 FICHIER SEQUENTIEL (SERIAL.ENC) 37
6.3.1 Format du fichier SERIAL.ENC 37
6.4 LE DOSSIER DU CATALOGUE DE LA S-57 FILE (CATALOG.031) 38
6.4.1 Structure et format du CATD-COMT 39
6.4.1.1 Encodage des cellules annulées (voir aussi les sections 6.2.3 et 6.2.3.1) 39
6.5 GESTION DE LA MISE A JOUR DES ENC T 40
6.5.1 Dossier STATUS.LST 40
6.5.1.1 Etat du format en-tête 40
6.5.1.2 Etat du format enregistrement 40
6.6 LE DOSSIER README DE LA S-57 (README.TXT) 41

7 STRUCTURE DE REPERTOIRE ET DE FICHIER 43

7.1 INTRODUCTION 43
7.2 GESTION DE FICHIER DE LA S-57 43
7.3 STRUCTURE DE FICHIER 43
7.4 DENOMINATION DE FICHIER ET DE DOSSIER 43
7.5 SUPPORT NUMERIQUE POUR L'ENSEMBLE DES DONNEES D'ECHANGE 43
7.5.1 CD-ROM 43
7.5.1.1 Définitions de dossier 44
7.5.2 Memoire de grande capaicté 44
7.5.3 Services en ligne 45

8 PROCESSUS DE L'ADMINISTRATEUR DU DISPOSITIF 46

8.1 ADMINISTRATEUR DU DISPOSITIF DE PROTECTION DES DONNES 47
8.2 PROCESSUS DE L'ADMINISTRATEUR DU DISPOSITIF 47
8.3 CREATION DE PAIRE DE CLES DE PREMIER NIVEAU 47
8.3.1 Création des paramètres PQG 47
8.3.2 Création de la clé privée 48
8.3.3 Création de la clé publique 48
8.4 CREATION ET PUBLICATION DU CERTIFICAT NUMERIQUE DE LA SA (X509v3) 48
8.4.1 UMise à jour du certificat numérique X509v3 de SA (clé publique) 48

8.5 PROCESSUS DES DEMANDES DE FOURNISSEURS ET DE FABRICANTS DE DONNEES 49
8.5.1 Processus de demande des fournisseurs de données pour un certificat de fournisseurs de données 49
8.5.1.1 Authentification du fichier de clé auto-signée (SSK) 49
8.5.1.2 Création du certificat de fournisseur de données 49
8.5.1.3 Authentification du certificat bde fournisseur de sonnées signé par le SA 50
8.5.1.4 Gestion des certificats de fournisseurs de données 50
8.5.2 Processus des demandes des fabriquants 51
8.5.2.1 Publication et gestion des codes de fabricant pour la S-63 51
8.5.2.2 Publication des listes M_ID et M_KEY aux fournisseurs de données 51
8.6 DONNEES D'ESSAI POUR LA S-63 51
8.7 ADMINISTRATEUR DU DISPOSITIF – PROCEDURES DE SECURITE RELATIVES A L'ASSURANCE QUALITE (QA) 51
8.7.1 Documentation 51
8.7.2 Gestion du contrat de confidentialité 51
8.7.3 Audit des registres de sécurité 51
8.7.4 Création des M_IDs et M_KEYs 52
8.7.5 Création des clés de signature numérique (clés privées et publiques) 52
8.7.6 Acceptation des clés auto-signées (SSK) 52
8.7.7 Création des certificats de fournisseur de données (DS) 52
8.7.8 Création de chaînes aléatoires 52
8.7.9 Remise des M_ID et M_KEY 53

9 PROCESSUS DE FOURNISSEUR DE DONNES 55

9.1 VUE D'ENSEMBLE 55
9.2 PROCESSUS DU FOURNISSEUR DE DONNEES 55
9.3 PROCESSUS DE CERTIFICATION 55
9.3.1 Production de paire de clé publique/privée 55
9.3.1.1 Création des paramètres de signature PQG 56
9.3.1.2 Création du fichier de clé privée 56
9.3.1.3 Création du fichier de clé publique 56
9.3.2 Création de clé auto-signée de fournisseur de données (SSK) 57
9.3.2.1 Signature de clé publique et émission de SSK 57
9.3.2.2 Authentification/Validation de SSK de fournisseur de données 57
9.3.2.3 Archivage de clé auto-signée 57
9.3.3 Validation des certificats 57
9.3.3.1 Authentification du certificat numérique X509 de SA 57
9.3.3.2 Authentification du certificat de fournisseur de données signés par le SA 58
9.3.3.3 Archivage du certificat de fournisseur de données signé par le SA 58
9.4 PROCESSUS DE GESTION DES DONNEES 59
9.5 CHIFFREMENT, COMPRESSION ET PROCESSUS DE SIGNATURE DES ENC 59
9.5.1 Gestion du chiffrement des clés de cellule (ECK) 59
9.5.1.1 Format de clé de cellule 60
9.5.2 Compression du fichier ENC (fichiers de base ou mise à jour) 60
9.5.3 Chiffrement des dossiers ENC 60
9.5.3.1 Fichier de base de cellule 60
9.5.3.2 Fichier de mise à jour des ENC 60
9.5.4 Signature du fichier ENC (Cellule de base ou mise à jour) 60
9.5.5 Publication de données ENC chiffrées pour la S-63 61
9.6 PROCESSUS DE L'ACCORD DE LICENSE 61
9.6.1 Décryptage du permis d'utilisateur 61
9.6.2 Création du permis de cellule 62
9.6.3 Publication de licenses pour ENC 64
9.7 PROCEDURES DE SECURITE RELATIVES A L'ASSURANCE QUALITE – FOURNISSEUR DE DONNEES 63
9.7.1 Information sur le dispositif de protection des données 64
9.7.2 Essai de conformité du système 64
9.7.3 Archivage des M_IDs et M_KEYs 64
9.7.4 Acceptation et contrôle du certificat numérique de SA (et clé publique) 64
9.7.5 Création de clés numériques de signature (Clés publique et privée) 64
9.7.6 Acceptation du certificat de fournisseur de données de la part du SA 64
9.7.7 Création de clés de cellule 64

9.7.8 Compression, chiffrement et signature de données S-57 64
9.7.9 Création de valeurs aléatoires 65
9.7.10 Création de permis de cellule 65
9.7.11 Déchiffrement des permis d'utilisateur 65

10 PROCESSUS DU FABRICANT ET DU CLIENT UTILISATEUR DE DONNEES 66

10.1 CLIENTS UTILISATEURS DE DONNEES 67
10.2 FABRICANTS (OEMS) 67
10.3 PROCESSUS DU FARICANT ET DU CLIENT UTILISATEUR DE DONNEES 67
10.4 CREATION DU PERMIS D'UTILISATEUR POUR LE CLIENT UTILISATEUR DE DONNES 68
10.5 INSTALLATION DU PERMIS DE CELLULE POUR ENC 68
10.5.1 Contrôle du dossier de permis de cellule 69
10.5.2 Contrôle du format de permis de cellule 69
10.5.3 Contrôle du HW_ID 69
10.5.4 Contrôle de la somme de contrôle du permis de cellule 69
10.5.5 Contrôle de la date d'expiration du permis de cellule 70
10.5.6 Contrôle de l'ID du fournisseur de données 70
10.6 CONTROLE DE L'AUTHENTIFICATION ET DE L'INTEGRITE DES ENC 71
10.6.1 Authentification/Vérification du certificat numérique de SA 71
10.6.1.1 Contrôle manuel de la clé publique de SA 72
10.6.2 Authentification du certificat de fournisseur de données signé par la SA 73
10.6.2.1 Authentification par rapport au certificat de fournisseur de données non signé par le SA 73
10.6.3 Authentification du fichier de cellule ENC 74
10.7 DECHIFFREMENT DES FICHIERS DE CELLULE DE BASE ET DE MISE A JOUR ENC 75
10.7.1 Contrôler l'état de l'abonnement des permis installés 75
10.7.1.1 Contrôler si l'abonnement a expiré dans un permis de cellule (avertissement requis) 76
10.7.1.2 Contrôler l'état de l'abonnement – (avertissement de 30 jours requis) 77
10.7.2 Déchiffrement des clés de cellule dans un permis de cellule 77
10.7.3 Déchiffrement des fichiers de cellule de base et de mise à jour ENC 78
10.7.4 Décompression de fichier ENC (cellule de base ou mise à jour) 78
10.8 AVERTISSEMENTS PERMANENTS DU CLIENT FOURNISSEUR DE DONNEES 78
10.8.1 Permis ENC expirés 80
10.8.2 Données SENC périmées 80
10.9 PROCEDURES D'ASSURANCE QUALITE – CLIENT UTILISATEUR DE DONNEES 80
10.9.1 Acceptation et contrôle du certificat numérique de SA (et clé publique) 80
10.9.2 Création du permis d'utilisateur 80
10.9.3 Vérification du certificat de fournisseur de données 80
10.9.4 Validation des permis de cellule 80
10.9.5 Authentification et déchiffrement des informations ENC 81
10.10 PROCEDURES D'ASSURANCE QUALITE –FABRICANTS (OEMS) 81
10.10.1 Contrat de confidentialité 81
10.10.2 Essai de conformité du système 81
10.10.3 Stockage des M_IDs et des M_KEYs 81
10.10.4 Création des HW_IDs 81
10.10.5 Enregistrement des HW_IDs 81

11 CODES D'ERREUR ET EXPLICATIONS DE LA S-63 83

ANNEXE A A LA S-63 87

1 OBJECTIF 89

2 RESPONSABILITE 89

2.1 BESOIN D'UN CERTIFICAT DE FOURNISSEUR DE DONNEES 89
2.2 SERVICES HYDROGRAPHIQUES ET ORGANISATIONS RENC 89
2.3 SERVICES NON-HYDROGRAPHIQUES ETORGANISATIONS NON-RENC 89
2.4 BUREAU HYDROGRAPHIQUE INTERNATIONAL 89

3 DEFINITIONS 89

3.1 REFERENCES 89

4 PROCEDURE 90
4.1 RENSEIGNEMENT DES FORMULAIRES ET PIECES JOINTES 90
4.2 AUTORISATION NECESSAIRE 90
4.3 ORGANISATION DONT DEPEND L'AUTORISATION 90
4.4 SOUMISSION DE FORMULAIRE DE DEMANDE AU BHI 90
4.5 VALIDATION DE LA DEMANDE DE CERTIFICAT 90
4.6 CREATION DU CERTIFICAT DE FOURNISSEUR DE DONNEES 90
5 EVALUATION DE LA QUALITE 90
ANNEXE B A LA S-63 93
1 OBJECTIF 95
2 RESPONSABILITE 95
2.1 OEMS 95
2.2 BUREAU HYDROGRAPHIQUE INTERNATIONAL 95
3 DEFINITIONS 95
3.1 REFERENCES 95
4 PROCEDURE 95
4.1 RENSEIGNEMENT DU FORMULAIRE DE DEMANDE 95
4.2 VERIFICATION DU FORMULAIRE DE DEMANDE 96
4.3 VERIFICATION DU CONTRAT DE CONFIDENTIALITE SIGNE 96
4.4 CONFIRMATION D'ESSAI REUSSI AVEC LES DONNEES D'ESSSAI DE LA S-63 96
4.5 CONTROLE QUE LE FABRICANT N'A PAS DE M_ID ET DE M_KEY 96
4.6 CREATION DE M_ID ET DE M_KEY 96
4.7 INFORMATION SUR LES NOUVELLES M_ID ET M_KEY 96
4.8 INFORMATION DE L'OEM SUR LES PROBLEMES RELATIFS A LA DEMANDE 97
5 EVALUATION DE LA QUALITE 97
APPENDICE 1 A LA S-63 [ENSEMBLE DE DONNEES D'ESSAI DE LA S-63] 99
1 INTRODUCTION 101
2 ORGANISATION DES DEFINITIONS D'ESSAI ET DES DONNEES D'ESSAI 101
2.1 DEFINITIONS D'ESSAI 101
2.2 DONNEES D'ESSAI 102
2.3 CONDITIONS D'UTILISATION DES DONNEES D'ESSAI 102
5.1.1 2.3.1 Conditions de fourniture des données 102
5.1.2 2.3.2 Exonération de responsabilité 102
APPENDICE 2 A LA S-63 [MEDIA DE GRANDE CAPACITE] 103
1 INTRODUCTION 105
2 VUE D'ENSEMBLE DES MEDIA 105
2.1 TYPES DE MEDIA 105
2.2 DOSSIER MEDIA ET STRUCTURE DE FICHIERS 105
2.2.1 Fichier média additionnel 106
2.3 IDENTIFICATION DES MEDIA 106
2.3.1 Immatriculation des média 106
3 FORMATS DE FICHIERS MEDIA 107
3.1 LISTE DE PRODUITS (PRODUCTS.TXT) 107
3.2 LISTE DE MEDIA (MEDIA.TXT) 107
3.2.1 Format des en-tête 107
3.2.2 Format des enregistrements média 108

4 GESTION DE MEDIA (FOURNISSEUR DE DONNEES) 109
5 GESTION DE MEDIA (CLIENTS UTILISATEURS DE DONNEES) 110
5.1 AVERTISSEMENTS MEDIA 110

GLOSSAIRE

Glossaire de termes relatif au dispositif de protection des données de la S-63

Blowfish	Algorithme de chiffrement utilisé par le dispositif de protection
Clé de cellule	Clé utilisée pour produire des ENC chiffrées, et nécessaire pour déchiffrer les informations ENC chiffrées.
Permis de cellule	Forme chiffrée de la clé de cellule, créée spécialement pour un utilisateur précis
Client utilisateur de données	Terme utilisé pour représenter l'utilisateur final qui reçoit les informations ENC chiffrées. Le client utilisateur de données utilisera un logiciel d'application (ECDIS par exemple) pour exécuter une grande partie des opérations spécifiées au sein du dispositif. Typiquement, un utilisateur d'ECDIS.
Fournisseur de données	Terme utilisé pour représenter une organisation qui produit des ENC chiffrées ou qui publie des permis de cellule à l'intention des utilisateurs finaux.
M_ID	ID unique assignée par le SA à chaque fabrication. Les fournisseurs de données l'utilisent pour identifier quelle M_KEY il faut utiliser lors du déchiffrement du permis d'utilisateur
M_KEY	Clé à ID unique du fabricant d'ECDIS fournie par le SA au fabricant. Elle est utilisée par le fabricant pour chiffrer le HW_ID lors de la création du permis d'utilisateur
HW_ID	ID unique assignée par un fabricant à chaque mise en oeuvre de son système. Cette valeur est chiffrée en utilisant la M_KEY unique du fabricant et elle est fournie au client utilisateur de données en tant que permis d'utilisateur. Cette méthode permet aux clients fournisseurs de données d'acheter des licenses pour déchiffrer les cellules ENC .
SA	Administrateur du dispositif
SHA-1	Algorithme haché sécurisé [3]
SSK	Clé auto-signée (Dossier de certificat auto-signé)
Permis d'utilisateur	Formulaire chiffré de HW-ID identifiant uniquement le système ECDIS

Termes cartographiques

ECDIS	Système de visualisation des cartes électroniques et d'information, tel que défini par l'OMI
ENC	Carte électronique de navigation telle que définie par les Spécifications de produit ENC [1].
S-57	Norme de transfert pour les ENC définie par l'OHI
SENC	Système de carte électronique de navigation (Il s'agit du format interne auquel le fabricant convertit les données lorsqu'ils les importent.)

Organisations

ECC	Centre de carte électronique AS (www.ecc.as)
SH	Service hydrographique (par exemple le fournisseur de données)
BHI	Bureau hydrographique international.
OHI	Organisation hydrographique internationale
OMI	Organisation maritime internationale
RENC	Centre régional de coordination ENC intégrant dans un seul service (par exemple le fournisseur de données) les ENC provenant de plusieurs SH.
SH du RU	Service hydrographique du Royaume-Uni www.ukho.gov.uk)

Termes informatiques

CRC	Contrôle cyclique par redondance
Dongle	Il y est souvent fait référence en tant que système mécanique codé de façon sécurisée. C'est un système mécanique fourni par le fabricant qui a un unique identificateur (HW_ID) stocké de façon sécurisée.
XOR	OU exclusif

Page laissée en blanc intentionnellement

1. INTRODUCTION

La publication "S-63 Dispositif de protection des données de l'OHI", appelée plus loint "le dispositif" décrit la norme recommandée pour la protection des informations ENC. Elle définit les dispositions de sécurité et les procédures opérationnelles qui doivent être respectées afin que le dispositif de protection des données puisse être exploité correctement et elle fournit les spécifications nécessaires aux participants pour la construction de systèmes conformes avec la norme S-63 et la diffusion des données d'une manière sécurisée et commecialement viable.

Le dispositif de protection des données a été préparé par le groupe consultatif sur le dispositif de protection des données (DPSWG) de l'Organisation hydrographique internationale (OHI). La norme S-63 est basée sur le dispositif de protection développé et exploité par Primar et Primar-Stavanger dans le cadre de leur service de fourniture d'ENC protégées. Le Centre de cartes éléctroniques AS et le Service hydrographique du Royaume-Uni ont été les premières organisations contributrices..

La norme a été adoptée en tant que norme officielle de l'OHI par les Etats membres de l'OHI en décembre 2002 (LC de l'OHI 66, 2002). Elle définit les rôles et les responsabilités en matière de protection des données ENC produites par les Services hydrographiques nationaux et distribués aux clients utilisateurs de systèmes ECS/ECDIS.

1.1 Description générale

Ce document précise la méthode de protection des informations ENC ainsi que la préservation de l'intégrité du service ENC avec plusieurs services de données pour une large base de clients utilisateurs de données. La protection des données a trois objectifs :

1. **Protection contre le piratage:** Empêcher la copie non autorisée des données en chiffrant les informations ENC.
2. **Accès sélectif:** Limiter l'accès aux informations ENC aux seules cartes pour lesquelles le client a obtenu les permis nécessaires
3. **Authentification:** Fournir l'assurance que les données ENC proviennent d'une source autorisée

La protection contre le piratage et l'accès sélectif sont obtenus par le chiffrement des informations ENC et la fourniture de permis de cellule pour les déchiffrer. Les fournisseurs de données chiffreront les données ENC fournies par les pays producteurs avant de les remettre au client utilisateur de données. Les ENC chiffrées sont ensuite déchiffrées par l'ECS/ECDIS avant d'être reformatées et importées dans le SENC. L'authentification est fournie par les signatures numériques des données.

Le dispositif ne répond pas précisémment à la question de savoir comment l'ENC ou le SENC peuvent être protégés dans le cadre d'une application d'utilisateur final. La responsabilité en incombe au fabricant.

Le dispositif permet la distribution en masse des ENC chiffrées sur support rigide (par exemple CD-ROM ou DVD) et tous les clients qui possèdent une licence valide contenant un ensemble de permis peuvent y accéder et l'utiliser. L'accès sélectif aux cellules individuelles se fait par la fourniture aux usagers d'un ensemble autorisé de permis contenant les clés de cellules chiffrées. Cette licence est créée au moyen d'un identifiant rigide unique du système et est unique pour chaque client utilisateur de données. En conséquence les licences ne peuvent être échangées entre clients fournisseurs de données individuels.

Le dispositif utilise un algorithme de compression dans le but de réduire la dimension de l'ensemble de données. Les données ENC déchiffrées contiennent un grand nombre d'informations répétitives, par exemple les informations coordonnées. La compression est en conséquence toujours utilisée avant que l'information ENC ne soit chiffrée par le fournisseur de données et la décompression après déchiffrement sur le système du client utilisateur de données (en principe ECS/ECDIS).

1.2 Participants au dispositif

Il existe plusieurs types d'utilisateurs du dispositif, ce sont les suivants :

- L'Administrateur du dispositif (SA) : il n'en existe qu'un.
- Le fournisseur de données (DS) : il peut y en avoir plusieurs.
- Le client utilisateur de données (DC) : il y en a beaucoup.
- Le fabricant (OEM) : il y en a beaucoup.

Vous trouverez ci-dessous une explication plus détaillée de ces termes :

1.2.1 Administrateur du dispositif

L'Administrateur du dispositif (SA) est le seul responsable de la mise à jour et de la coordination du dispositif. Le rôle de l'Administrateur est assuré par le Bureau hydrographique international (BHI), en tant que secrétariat de l'OHI, au nom des Etats membres.

Le SA est responsable du contrôle des adhésions au dispositif et du respect par tous les participants des procédures définies. Le SA met à jour les clés de chiffrement dites « top level » qui sont utilisées pour la mise en application du dispositif de protection des données de la S-63 et c'est la seule instance qui peut attesté de l'identité des autres participants au dispositif.

Le SA est aussi le garant de toute la documentation relative au dispositif de protection des données de la S-63.

1.2.2 Fournisseurs de données

Les fournisseurs de données sont responsables du chiffrement et de la signature des données ENC selon les procédures et les processus définis dans le dispositif. Les fournisseurs de données publient les licences ENC (permis) de façon à ce que les clients utilisateurs de données, en possession de permis d'utilisateur valides, puissent déchiffrer les données ENC.

Les fournisseurs de données utiliseront les informations M_KEY et HW_ID, telles que fournies par le SA, pour produire les clés de cellule ENC chiffrées destinées à chaque installation spécifique. Même si les clés de cellule utilisées pour chiffrer chaque cellule sont identiques, elles seront chiffrées en utilisant une HW_ID unique et en conséquence ne pourront pas être transférées à d'autres ECDIS provenant du même fabricant.

Les services hydrographiques, les distributeurs à valeur ajoutée et les organisations RENC sont des exemples de fournisseurs de données.

1.2.3 Clients utilisateurs de données

Les clients utilisateurs de données sont les utilisateurs des informations ENC et recevront des informations protégées en provenance des fournisseurs de données. Le logiciel d'application du client utilisateurs de données (Système OEM) est responsable de l'authentification des signatures numériques des ENC et du déchiffrement des informations ENC conformément aux procédures définies dans le dispositif.

Les navigateurs disposant de systèmes ECDIS/ECS sont des clients utilisateurs de données potentiels.

Le dispositif de protection n'empêche pas les agents ou les distributeurs de fournir des services en matière de données à leurs clients. Les contrats et les structures nécessaires pour ce faire ne rentrent pas dans le domaine d'application de ce document. Ce dernier ne contient que les spécifications techniques destinées à produire des services et des systèmes de données conformes à la S-63.

1.2.4 Fabricants

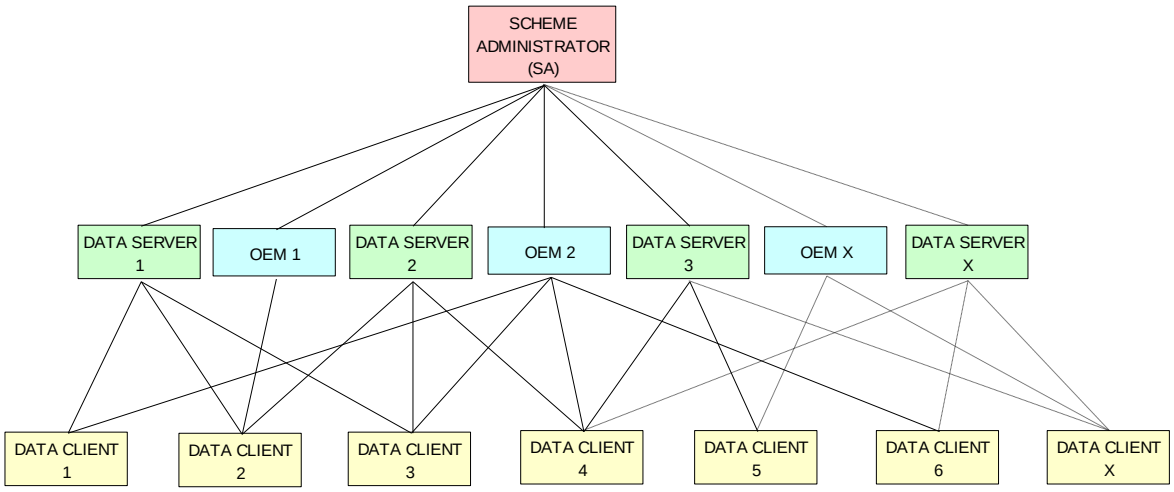
Les fabricants ayant souscrit au système de protection des données de l'OHI doivent construire un logiciel d'application selon les spécifications établies dans ce document et le vérifier et le valider selon les termes choisis par le SA. La norme S-63 contient des données d'essai pour la vérification et la validation des applications des fabricants. Le SA fournira aux fabricants dont la demande a été acceptée leur clé de fabricant unique et leur identification (M_KEY et M_ID).

Le fabricant doit fournir un mécanisme sécurisé à l'intérieur de son système de logiciel pour identifier chaque installation d'utilisateur final. Le dispositif nécessite que chaque installation ait un identificateur unique de matériel. (HW_ID).

L'application du logiciel pourra déchiffrer les clés de cellule en utilisant le HW_ID stocké dans les appareils sécurisés ou non sécurisés qui sont reliés à l'application ou programmés au sein de celle ci pour, par la suite, déchiffrer et décompresser les données ENC. La valeur CRC contenue dans les ENC peut alors être vérifiée afin d'établir l'intégrité des données sous-jacentes relatives à la S-57.

1.2.5 Relations entre les participants à la S-63

L'Administrateur du dispositif, dont il ne peut y avoir qu'un seul représentant, authentifie l'identité des autres participants au sein du dispositif. Tous les fournisseurs de données et les fabricants de système doivent faire une demande au SA pour participer au dispositif et, après acceptation de la demande, des informations spécifiques qui seront uniques pour eux leur seront fournies. Les clients utilisateurs de données sont des clients des fournisseurs de données et des fabricants avec lesquels les fournisseurs de données apportent des services relatifs aux données et les clients utilisateurs de données l'équipement nécessaire pour déchiffrer et visualiser ces services.



IHO S-63 Data Protection Scheme Relationships

1.3 Références

[1] S-57 Edition 3.1: Normes de l'OHI pour le transfert de données hydrographiques numériques, Bureau hydrographique international (www.iho.int)

[2] Digital Signature Standard (DSS), FIPS Pub 186 (www.itl.nist.gov/div897/pubs/fip186.htm)

[3] Secure Hash Standard (SHA), FIPS Pub 180-1 (www.itl.nist.gov/div897/pubs/fip180-1.htm)

[4] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. X.509 version 3 International Telecommunication Union.

[6] ZIP File Format Specification, PKWare Inc.

[7] DES Modes of Operation, FIPS Pub 81(www.itl.nist.gov/fipspubs/fip81.htm)

[8] RFC 1423: Privacy Enhancements for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers (ftp://ftp.isi.edu/in-notes/rfc1423.txt)

[9] Blowfish encryption algorithm, B. Schneier, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204. (www.counterpane.com)

[10] Algorithme de la somme de contrôle CRC32. Technologies de l'information -- Télécommunications et échange d'information entre systèmes -- Procédures de commande de liaison de données à haut niveau (HDLC). ISO/CEI 13239:2002.

1.4 Compatibilité avec les précédentes versions

La présente édition de la S-63 utilise les mêmes algorithmes et les mêmes formats et contenus de fichier que le dispositif de sécurité exploité par Primar, Primar-Stavanger et la version 1.0 de la S-63 de l'OHI. Cette version de la norme S-63 de l'OHI a été amendée en vue de fournir de meilleures définitions et une explication sur l'exploitation du dispositif de protection.

Un ensemble de données d'essai défini a été produit et doit être utilisé par les fabricants pour vérifier et valider les mises en application du dispositif de protection des données de la S-63 au cours de l'auto-certification.

La Version 1.1 de la norme a été produite en tenant compte de l'expérience acquise par les fournisseurs de données et les fabricants d'ECS/ECDIS au cours de l'exploitation de la version 1.0 du dispositif. Cette version vise à définir la norme plus clairement en supprimant les répétitions et les ambiguïtés éventuelles. Elle contient également des mécanismes additionnels qui permettront aux fabricants de rendre leurs systèmes plus intituitifs pour les utilisateurs d'ECS/ECDIS. Les révisions apportées à la norme sont listées ci-dessous :

1. Suppression des répétitions inutiles
2. Spécification relative à la manière et aux conditions dans lesquelles certains fichiers doivent être utilisés.
3. Suppression de l'interdépendance du permis sur l'édition de la cellule.
4. Information additionnelle pour permettre aux clients utilisateurs de données de gérer les données 5. ENC de façon plus efficace
5. Identification d'une stratégie de chargement afin de permettre un chargement plus efficace des ENC chiffrées.

Les fournisseurs de données ont la responsabilité de fournir des services qui sont rétrocompatibles.

1.5 Structure du Document

Le corps principal du document peut généralement être divisé en quatre parties. La première partie décrit les composantes essentielles du dispositif ainsi que leur objectif et leur agencement. La deuxième partie identifie de quelle manière l'ensemble des composantes est réuni dans l'ensemble de données d'échange de la S-63. La troisième partie souligne les rôles et les responsabilités de chaque type d'utilisateur participant au dispositif. Finalement, une section définit les différents messages d'erreur et d'avertissements qui doivent être visualisés par le client utilisateur de données lorsque les conditions décrites apparaissent.

Document principal:

1. Composantes du dispositif:
   - Section 2 Compression des données
   - Section 3 Chiffrement des données
   - Section 4 Accord de licence relatif aux données
   - Section 5 Authentification des données
   - Section 6 Gestion des données

2. Format et structure de l'ensemble des données d'échange
   - Section 7 Structures du répertoire et des fichiers

3. Processus relatifs aux participants au dispositif de la S-63
   - Section 8 Processus relatif à l'Administrateur du dispositif
   - Section 9 Processus du fournisseur de données
   - Section 10 Processus des fabricants et des clients utilisateurs de données

4. Messages d'erreur et d'avertissements de la S-63
   - Section 11 Codes d'erreur et explications de la S-63

Sections additionnelles:

- Annexe A à la S-63 : Procédure de demande de certificat de fournisseur de données
- Annexe B à la S-63 : Procédure de demande d'informations du fabricant.

Appendices:

- L'Appendice 1: Contient une définition des données d'essai disponibles qui peuvent être utilisées en vue d'obtenir une conformité totale avec tous les aspects du dispositif de protection des données.
- L'Appendice 2: Définit de quelle manière les ensembles de données d'échange fournis par les fournisseurs de données seront stockés en utilisant des mémoires de grande capacité comme les DVID ou les clés USB.

1.6 Tenue à jour

Les changements à cette norme seront conformes aux "Principes et procédures pour la modification des normes et des spécifications de l'OHI", tels qu'approuvés par la 18e réunion du CHRIS (Cairns, Australie, septembre 2006).

1.7 Assistance

Une assistance pour l'utilisation et la mise en oeuvre de cette norme est fournie aux utilisateurs par les membres du DPSWG de l'OHI, *via* une discussion du dispositif de sécurité sur l'Open ECDIS Forum. (www.openecdis.org). De plus, un récapitulatif des questions les plus fréquemment posées (FAQ) est mis à jour par le BHI dans la section ECDIS du site web de l'OHI (www.iho.int).

Page laissée en blanc intentionnellement

2. COMPRESSION DES DONNEES

2.1 Vue d'ensemble

Du fait de sa structure, un fichier ENC contiendra des schémas répétitifs d'informations. Des exemples en sont donnés par la numérotation consécutive de l'indentificateur de l'élément objet ou par de petites variations dans les informations coordonnées à l'intérieur d'un fichier ENC. Les données ENC en conséquence répondent bien à la compression avec des réductions de taille entre 30% et 60%, rédduisant grandement le coût de transfert des données ENC vers leur destination finale. Seuls les fichiers ENC (base et mise à jour) sont compressés. Les fichiers ENC sont toujours compressés avant d'être chiffrés car l'efficacité de tout algorithme de compression repose sur l'existence de contenus de données structurés.

2.2 Algorithme de compression

Le dispositif de sécurité utilise l'algorithme ZIP[1] [6] pour compresser et décompresser les données ENC. Cela est identique à l'algorithme utilisé dans un grand nombre d'applications commerciales, par exemple WinZip, PKZIP. Les éventuels fournisseurs de données et les fabricants doivent tenir compte du fait que dans le passé des erreurs se sont produites lorsque les fournisseurs de données ont compressés les données et qu'elles sont interprétées par les applications communes de l'algorithme ZIP en tant que données « texte ». Si les données sont décompressées au moyen de paramètres incorrects elles peuvent corrompre le fichier ENC et mener à l'échec des contrôles d'intégrité. Il est conseillé aux fournisseurs de données et aux fabricants d'appliquer la compression/décompression au sein de leurs systèmes.

2.3 Fichiers compressés

Le dispositif de sécurité compresse seulement les fichiers de cellule de base ENC et les fichiers de mise à jour. Aucun autre fichier dans l'ensemble de données d'échange S-57 ne sera compressé.

[1] http://en.wikipedia.org/wiki/ZIP_%28file_format%29

Page laissée en blanc intentionnellement

3. CHIFFREMENT DES DONNEES

3.1 Quelles données sont chiffrées?

Un seul algorithme de chiffrement est utilisé dans le dispositif. Seules les données de fichiers de cellule de base et de mises à jour contenues dans l'ensemble d'échange de données de la S-57, par exemple les fichiers texte ou image demeurent non chiffrés. D'autres informations du dispositif qui sont chiffrées incluent le HW_ID du système du fabricant qui est chiffré et fourni au client utilisateur de données sous la forme d'un permis d'utilisateur.

Les clés de cellule utilisées pour chiffrer les fichiers de données ENC sont elles-mêmes chiffrées par le fournisseur de données et fournies aux clients utilisateurs de données en tant que permis de cellule. Les informations concernant l'algorithme de chiffrement sont disponibles à la section 3.2.3.

3.2 Comment les données sont elles chiffrées ?

Chaque fichier individuel d'ENC est chiffré en utilisant la clé de cellule. La même clé de cellule est utilisée pour chiffrer toutes les mises à jour émises pour cette édition de l'ENC. Le dispositif cependant permet d'accroître et de changer les clés de cellule à la discrétion du fournisseur de données. Les clés de cellules sont délivrées sous la forme de permis de cellule au client utilisateur de données.

3.2.1 Chiffrement des informations ENC

Les informations ENC (cellules de base et mises à jour) sont chiffrées en utilisant une clé de 40-bits.

3.2.2 Chiffrement des autres informations relatives au dispositif de protection

Le contenu du permis d'utilisateur et du permis de cellule sont chiffrés en utilisant une clé de 48 bits.

3.2.3 Algorithme de chiffrement – Blowfish

Le dispositif de protection chiffre toutes les informations référencées en 3.1 en utilisant l'algorithme Blowfish [9]. L'algorithme est non breveté et relève du domaine public (www.counterpane.com). Blowfish est un algorithme de chiffrement par bloc qui travaille par quantités de 64 bits (8 octets). Il est nécessaire que les données source soient complétées si elles ne sont pas des multibles de 8 octets. Le dispositif de protection utilise l'algorithme de remplissage "DES in CBC Mode" padding algorithm defined in [8] whenever any data sources must be padded. This complies with the ECB (Electronic Code Book) mode of DES [7].

Page laissée en blanc intentionnellement

4. ACCORD DE LICENCE RELATIF AUX DONNEES

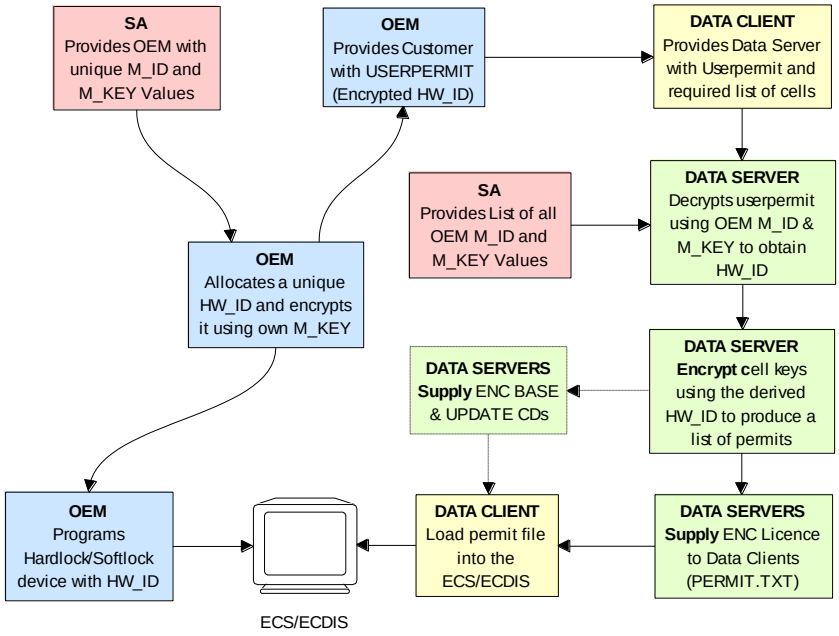
4.1 Introduction

Les clients utilisateurs de données n'achètent pas les données ENC mais sont autorisés à les utiliser. L'accord de licence est la méthode que les fournisseurs de données utilisent pour donner aux clients utilisateurs de données l'accès sélectif aux cellules ENC pendant une période donnée.

Pour une exploitation efficace du dispositif, il doit y avoir un moyen par lequel les clients fournisseurs de données peuvent dévérouiller les cellules ENC chiffrées. Pour déverouiller les données, le système des clients utilisateurs de données doit avoir accès aux clés de cellule qui ont été utilisées pour chiffrer les cellules ENC. Ces clés sont remises au client utilisateur de données, chiffrées, dans un fichier de permis contenant un ensemble de permis de cellule. Ce sont ces permis de cellule qui contiennent les clés de chiffrement.

Pour rendre chaque ensemble de permis de cellule exclusif les clés de cellule doivent être chiffrées en utilisant quelque chose qui est unique au système des clients utilisateurs de données. Le fabricant attribue un identificateur unique (HW_ID) à chacun de leurs système et en fournit un exemplaire chiffré, sous la forme d'un permis d'utilisateur, à chaque client utilisateur de données. Le HW_ID est stocké dans le permis d'utilisateur chiffré.

Le fabricant chiffre le HW_ID avec sa propre clé unique de fabricant (M_KEY) de façon à ce que le HW_ID ne puisse pas être reproduit par un autre fabricant. Les fournisseurs de données ont accès aux clés de fabricant et peuvent donc déchiffrer le HW_ID stocké dans le permis d'utilisateur. Les fournisseurs de données chiffrent leurs clés de cellule avec le HW_ID des fabricants lorsqu'ils produisent un ensemble de permis de cellule. Ceci les rend uniques pour le client utilisateur de données et donc non transférables entre les systèmes des clients fournisseurs de données.



High Level ENC Licencing Diagram

4.2 Le permis d'utilisateur

Le permis d'utilisateur est créé par les fabricants et fourni aux clients utilisateurs de données dans le cadre de leur système de façon à ce qu'ils puissent obtenir des fournisseurs de données l'accès nécessaire aux ENC chiffrées. La composition et le format du permis d'utilisateur sont définis dans la section suivante.

Tous les clients utilisateurs de données possédant des systèmes capables de traiter les données, protégées par le dispositif S-63, doivent avoir un identificateur de matériel unique (HW_ID) intégré dans leur système final. Un tel HW_ID est souvent implémenté par une clé de protection mécanique (dongle) ou par d'autres moyens assurant l'identification unique de chaque installation.

Le HW_ID n'est pas connu des clients utilisateurs de données, mais le fournisseur du système de l'utilisateur fournira à ce dernier un permis d'utilisateur qui sera une version chiffrée HW_ID. Le permis d'utilisateur est créé en prenant le HW_ID attribué et en le chiffrant avec la clé du fabricant (M_KEY). Le HW_ID est chiffré au moyen de l'algorithme CRC32 et le résultat y est attaché. Finalement le fournisseur du système attache son identificateur de fabricant assigné (M_ID) jusqu'à la fin de la chaîne qui en résulte. Les valeurs de M_KEY et de M_ID sont fournies par l'administrateur système et sont uniques pour chaque fabricant qui fourni des systèmes compatibles avec la S-63.

Le client utilisateur de données a accès aux nouvelles informations en donnant son permis d'utilisateur au fournisseur de données qui établira des permis de cellules spécifiques au permis d'utilisateur. Etant donné que le permis d'utilisateur contient un M_ID de fabricant unique, ce dernier peut être utilisé par les fournisseurs de données pour déterminer quelle M_KEY utiliser pour déchiffrer le permis d'utilisateur. Les quatre derniers caractères du permis d'utilisateur forment la M_ID. Une liste des valeurs des M_KEY et M_ID du fabricant est publiée et mise à jour par l'Administrateur du système à tous les fournisseurs de données qui souscrive au dispositif. Cette liste sera mise à jour périodiquement au fur et à mesure que de nouveaux fabricants rejoignent le dispositif.

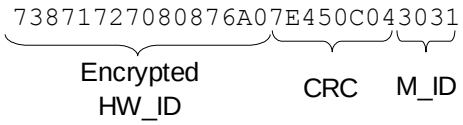
4.2.1 Définition du permis d'utilisateur

Le permis d'utilisateur est composé est composé de 28 caractères en langage ASCII avec format et longueur de champ obligatoires, à savoir :

HW_ID chiffrée	Somme de contrôle (CRC)	M_ID (ID fabricant)
16 caract. hex.	8 caract. hex.	4 caract.

Tout caractère alphabétique sera écrit en lettres capitales.

Example: Userpermit Structure



4.2.2 Format HW_ID

Le HW_ID est un nombre décimal de 5 octets défini par le fabricant OEM. Un tel HW_ID peut être implémenté par une clé de protection mécanique (dongle) ou par d'autres moyens assurant l'identification unique de chaque installation[2]. Le HW_ID doit être stocké à l'intérieur du système d'une manière sécurisée.

Le fabricant OEM doit assigner un HW_ID unique pour chaque installation. Il est recommandé que les HW_ID ne soient pas séquentiels.

Le HW_ID sera stocké sous forme chiffrée dans le permis d'utilisateur. Il est chiffré au moyen de l'algorithme Blowfish avec pour clé la M_KEY qui donne un nombre hexadécimal de 8 octets. Le HW_ID chiffré est donc représenté en format ASCII dans le permis d'utilisateur sous forme hexadécimale.

Exemple de HW_ID : `A79AB`
Exemple de HW_ID chiffré : `73871727080876A0`

[2] Le fabricant, avec l'autorisation du fournisseur de données, peut utiliser le même HW ID sur plus d'une unité.

4.2.3 Format de la somme de contrôle (CRC)

La somme de contrôle est constituée de 8 caractères hexadécimaux (4 octets). Elle est générée en prenant le HW_ID chiffré et en le convertissant en une chaîne de 16 caractères hexadécimaux. Cette dernière est hachée ensuite en utilisant l'algorithme CRC32 [10] et les 4 octets sont convertis en une chaîne de 8 caractères hexadécimaux. .

La somme de contrôle n'est pas chiffrée et permet de contrôler l'intégrité du permis d'utilisateur

La somme de contrôle dans l'exemple ci-dessus est : 7E450C04

4.2.4 Format M_ID

Le M_ID est un code alphanumérique de 2 caractères, exprimés en langage ASCII ; il est fourni par le SA. Le SA fournira à tous les fabricants autorisés la combinaison de leur propres clé de fabricant et identificateur uniques. Le fabricant doit protéger cette information.

Le SA fournira à tous les fournisseurs de données autorisés une liste complète de codes de fabricants au fur et à mesure que de nouveaux fabricants s'abonneront au dispositif. Ces informations sont utilisées par le fournisseur de données pour déterminer quelle clé (M_KEY) utiliser pour déchiffrer le M_ID). Le fabricant doit protéger cette information. Elle est utilisée par le fournisseur de données pour déterminer quelle clé (M_KEY) utiliser pour déchiffrer le HW_ID dans le permis d'utilisateur au cours de la création des permis de cellule du client utilisateur de données.

Le M_ID dans l'exemple ci-dessus est: 01 ou 3031 (ASCII)[3])

4.2.5 Format M_KEY

La M_KEY est un nombre hexadécimal de 5 octets fourni par le SA. Le fabricant utilise cette clé pour chiffrer le HW ID attribué lorsqu'il crée les permis d'utilisateurs. Le fabricant doit la stocker de façon sécurisée. Elle est utilisée par le fournisseur de données pour déchiffrer la HW_ID attribuée.

Exemple de M_KEY : 123AB ou 3132334142 (langage ASCII)

4.3 Le permis de cellule

Pour déchiffrer une cellule ENC le client utilisateur de données doit avoir accès à la clé de chiffrement (voir section 3.2) utilisée pour chiffrer celle-ci. Depuis que les clés de chiffrement sont seulement connues du fournisseur de données, il doit exister un moyen de diffuser cette information de manière protégée aux clients utilisateurs de données. Cette information est donnée par le fournisseur de données (par exemple RENC ou VAR) au client utilisateur de données sous une forme chiffrée appelée permis de cellule. Un fichier unique, nommé PERMIT.TXT (voir section 4.3.1) est fourni pour remettre le permis de cellule. Ce fichier peut contenir plusieurs permis de cellule à partir de la couverture ENC demandée par le client utilisateur de données.

Le fichier PERMIT.TXT sera remis soit sur support rigide soit en utilisant les services en ligne conformément aux procédures opérationnelles des fournisseurs de données. Ces procédures seront mises à la disposition des clients utilisateurs de données au moment où ils achèteront une licence.

Chaque enregistrement de permis de cellule contient également des champs additionnels qui sont fournis en vue d'aider les systèmes des fabricants à gérer la licence des clients utilisateurs de données et les fichiers provenant de plusieurs fournisseurs, voir section 4.3.3.

---

[3] Note: Le codage hexa peut n'être pas familier à certains lecteurs. Pour des raisons historiques, il a été conservé dans cette version de la norme. "1 2 3 4 5" est traduit par "31 32 33 34 35" parce que la base 16 du caractère « 1 » est 31 en language ASCII etc. Bien qu'entraînant une certaine confusion dans un premier temps, cette convention est utilisée de manière cohérente tout au long de la norme ainsi que dans les représentations hexadécimales et binaires de la norme. Pour les différencier, il y est fait référence en tant que « (ASCII) ».

Les clients utilisateurs de données peuvent obtenir une licence d'accès aux ENC en donnant au fournisseur de données leur permis d'utilisateur unique (voir 4.2). Les fournisseurs de données peuvent ensuite extraire le HW_ID du permis d'utilisateur en utilisant la M_KEY du client utilisateur de données et créer des permis de cellule spécifiques pour les clients. Le format d'un permis de cellule est décrit ci-dessous aux sections 4.3.2 et 4.3.3.

Etant donné que les permis de cellule sont délivrés pour un HW_ID spécifique, ils ne sont donc pas transférables entre les installations (systèmes du client utilisateur de données). Cette méthode consistant à relier le permis à l'installation soutient la production de CD-ROM génériquement chiffrés qui peuvent être distribués à tous les clients utilisateurs de données qui s'abonnent à un service.

Le système des clients utilisateurs de données déchiffre le permis de cellule en utilisant le HW_ID attribué qui est stocké de façon sécurisée en matériel ou en logiciel. Les clés de cellule déchiffrées peuvent ensuite être utilisées par le système pour déchiffrer la cellule ENC. Etant donné que plusieurs fournisseurs de données peuvent faire des fichiers de permis pour ENC dans leur service, il relève de la responsabilité du client utilisateur de données de gérer les fichiers de permis à partir des différents fournisseurs de données.

NOTE: Les fournisseurs de données devront continuer à fournir deux types de fichiers de permis (ENC.PMT & PERMIT.TXT) tels que décrits dans l'édition 1.0 de la S-63. Ceci devra se poursuivre jusqu'au moment où l'on pourra être sûrs que l'omission du fichier ENC.PMT ne compromettra pas l'utilisation sécurisée des anciens systèmes patrimoniaux. L'intervalle de temps nécessaire pour ce faire doit être convenu entre les parties prenantes. **Les fabricants de données** doivent faire en sorte que les nouvelles implémentations de leur logiciel ECDIS puissent fusionner les permis provenant de différents fournisseurs de données sans perdre les informations relatives au permis en n'utilisant que le fichier PERMIT.TXT file.

4.3.1 Le fichier de permis (PERMIT.TXT)

Le permis de cellule sera toujours fourni dans un fichier appelé PERMIT.TXT, le nom du fichier sera toujours en LETTRES CAPITALES ainsi que tout caractère alphabétique contenu dans le fichier. Le fichier est entièrement codé en langage ASCII[4] et comprend les trois sections suivantes :

Section	Description
En-tête	Ceci comprend la date de création du fichier et le format.
:ENC	Les permis ENC (officiels) en provenance du fournisseur de données sont listés dans cette section.
:ECS	Les permis ECS (non-officiels) en provenance du fournisseur de données peuvent être listés dans cette section.

Le fournisseur de données mettra à disposition des renseignements sur la façon dont les fichiers de permis seront mis à dispsotion, soit sur support rigide soit sur services en ligne. Le tableau suivant définit le contenu et le format de chaque section au sein des fichiers de permis séparés par des « nouvelles lignes [NL] »

[4] Les fabricants (OEM) doivent être conscients que tous les fichiers texte en langage ASCII produits par le dispositif peuvent contenir des marqueurs de fin de ligne ambigus tels que CR (retour chariot) ou CRLF (retour chariot avec saut de ligne) et doivent être en mesure de les traiter**.**

4.3.2 Le fichier de permis – Formats des en-têtes

Le tableau suivant définit le contenu et le format de chaque en-tête de section au sein du fichier de permis.

Section	Nom du champ	Valeur
Date et heure	:DATE	Le nom du champ, la date et l'heure sont séparés par un espace (S¨<h20>. La date sera indiquée sous la forme YYYYMMDD et l'heure sous la forme HH :MM en utilisant le cadran de 24 heures. . Exemple : :DATE 20050809 11 :11
Version métapermis	:VERSION	Nombre entier de 1 à 99 Il sera augmenté de 1 à chaque nouvelle version de la spécification de format du fichier de permis. L'édition 1.1 de la S-63 définit la valeur comme étant «2 ». Par exemple. :VERSION 2
Type de permis de cellule	:ENC	Le champ contient la définition des permis disponibles sous licence de distribution ENC du fournisseur de données. Le champ est identifiée par le label suivant en lettres capitales : ENC
Type de permis de cellule	:ECS	Le champ contient la définition des métapermis disponibles sous licence de distribution ECS du fournisseur de données. Le champ est identifié par le label suivant en capitales :ECS

```
Exemple:  :DATE 20080809 11:11
          :VERSION 2
          :ENC
          [Liste des permis de cellules ayant la licence pour ENC officielles
          :ECS
          [Liste des permis de cellules ayant la licence pour d'autres produits
                vectoriels]
```

4.3.3 Zones d'enregistrement des permis

L'enregistrement des permis de cellule est composé des sections suivantes séparées par des virgules :

Champ	Valeur
Permis de cellule	Tel que défini en sections 4.3.4 & 4.3.5
Indicateur du niveau de service	**0** pour le permis d'adhésion **1** pour le permis d'achat unique
Numéro d'édition [Optionnel]	Numéro de parution DSID-EDTN de la cellule ENC (pour fournisseurs de données seulement)
ID du fournisseur de données	2 caractères alphanumériques publiés par le SA
Commentaire	Champ texte libre pour commentaires sur le permis de cellule, etc..

NOTE: Le champ "Numéro d'Edition [Optionnel]" n'est plus obligatoire dans l'Edition 1.1 de la S-63. **Les fabricants** qui implémentent l'édition 1.1 ne doivent pas introduire dans leurs systèmes de dépendance entre le numéro d'édition d'ENC et la clé de cellule utilisée pour la chiffrer. *Les clients utilisateurs de données* doivent seulement vérifier s'il existe une clé de cellule valide dans la chaîne de permis. *Les fournisseurs de données* continueront à soutenir l'édition 1.0 des fichiers PERMIT.TXT jusqu'à ce qu'on puisse déterminer qu'elle n'est plus nécessaire.

4.3.4 Définition du permis de cellule

Le tableau suivant définit les champs contenus dans le permis de cellule ainsi que le but de chacun d'entre eux.

Champ	But
Nom de cellule	Le nom de cellule permet aux systèmes du client utilisateur de données de lier la clé de chiffrement correcte au fichier de cellule ENC chiffrée correspondant.
Date d'expiration	Indique la date à laquelle la licence du client utilisateur de données expire. Les systèmes doivent empêcher que de nouvelles cellules, des éditions ou des mises d'ENC soient créées après cette date.
Clé de cellule chiffrée 1 (ECK1)	ECK1 contient la clé de déchiffrement concernant la version actuelle de la cellule ENC.
Clé de cellule chiffrée (ECK2)	ECK2 contient la clé de déchiffrement à utiliser lorsque la clé de cellule sera réitérée. La future clé est contenue au sein du permis de cellule pour permettre aux fournisseurs de données de changer périodiquement la clé de cellule sans publier simultanément de nouveaux permis de cellule aux clients utilisateurs de données.
Somme de contrôle (CRC)	Cette valeur représente une protection contre une falsification ou une corruption accidentelle

4.3.5 Format de permis de cellule

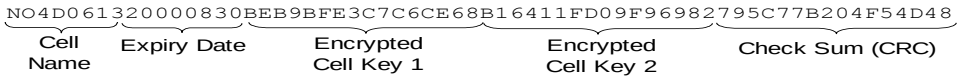
Le permis de cellule sera écrit en langage ASCII avec les formats et longueurs de champ obligatoires suivants :

Exemple:

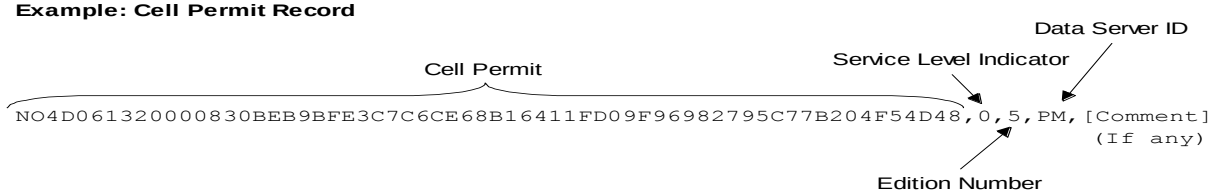
Champ	Caractère	Format
Nom de cellule	8	Une chaîne alphanumérique suivant la convention définie dans l'édition 3.1 de la S-57, Appendice B, section 5.6 pour les noms de cellules, à l'exclusion de l'extension de nom de fichier. Exemple : `NO4D0613`
Date d'expiration	8	Une chaîne numérique qui contient la date d'expiration de la licence pour chaque ENC au format `YYYYMMDD` Exemple : `20000830` (30 août 2000)
ECK1 & ECK2[5]	16	Les clés de cellule sont des nombres aléatoires de 5 octets – leurs représentations hexadécimales sont chiffrées en utilisant le Blowfish et ensuite convertis en nombre hexadécimaux dans le permis. **Note:** L'algorithme de chiffrement Blowfish permet de compléter les données chiffrées pour obtenir une longueur multiple de 8 octets. Ceci signifie que les clés de cellule chiffrées sont en fait d'une longueur de 8 octets, même si non chiffrées elles sont d'une longueur de 5 octets seulement (10 caractères hexadécimaux) Exemple: ECK1: `BEB9BFE3C7C6CE68` ECK2: `B16411FD09F96982`
Permis ENC Somme de contrôle	16	Il contient la somme de contrôle chiffrée pour le permis de cellule. Il est chiffré au moyen de l'algorithme avec le H_ID spécifique du client utilisateur de données et c'est un nombre de 8 octets. Cette somme de contrôle est chiffrée par opposition à la somme de contrôle non chiffrée du permis d'utilisateur. Exemple : La somme de contrôle ENC dans l'exemple suivant est : `795C77B204F54D48`

[5] Le permis de cellule contient deux champs qui fournissent au système du client utilisateur de données les clés de cellule nécessaires pour déchiffrer un fichier de cellule ENC spécifique. Ces champs peuvent contenir deux clés de cellule identiques ou deux clés de cellule différentes et ils peuvent être différents entre fournisseurs de données. Certains fournisseurs de données choisissent d'augmenter les clés de cellule uniquement si le dispositif de sécurité est modifié, d'autres préfèrent l'augmenter périodiquement conformément aux procédures en service. Le mécanisme concernant les fournisseurs de données qui produisent ces clés est décrit en détail à la section 9.5.1. Les fabricants (OEM) doivent prendre en compte que toute dépendance avec le numéro d'édition doit être supprimée de leurs systèmes dans l'édition 1.1 du dispositif.

Example: Cell Permit Field



Example: Cell Permit Record



4.3.6 Fichier de licence additionnel (Optionel)

Les fournisseurs de données peuvent souhaiter inclure un fichier additionnel au fichier PERMIT.TXT afin d'identifier le détenteur de licence et fournir des renseignements relatifs au système d'identification[6]. Ce fichier sera nommé **.LIC, où ** représente l'identification du fournisseur de données.

Les systèmes du client utilisateur de données peuvent avoir accès à ce fichier (s'il existe) pour afficher les renseignements relatifs à l'utilisateur et fournir les renseignements relatifs au permis d'utilisateur.

Le fichier contient un seul enregistrement comprenant les champs suivants :

Champ d'identification	Caractères	Notes
Détenteur de licence	40	Nom de la compagnie ou du particulier qui signe la licence.
Nom du navire	40	Optionnel. Ce champ peut être remplacé par des espaces.
Site fixe #1	240	Nom et adresse de la compagnie. Ce champ contient du texte en format libre décomposé en 6 sous-champs de 40 octets. Le texte ne croisera pas les limites des sous-champs.
Nom du système Hôte	40	Par exemple, principal, de secours, etc.
Permis d'utilisateur	28	Permis d'utilisateur hexadécimal
Type de licence	40	Indicateur de service, par exemple Service Primar Stavanger d'ENC
Données SH	36	Données pour SH / Agent / Distributeur.

Nombre total d'octets: 464

[6] Il peut être utile au cours du traitement des questions des clients utilisateurs de données d'avoir un accès direct aux renseignements relatifs au client tels que les renseignements concernant la licence et l'identification du fabricant. Les clients utilisateurs de données pourront fournir se fichier en même temps que la question pour réduire le délai de réponse.

Page laissée en blanc intentionnellement

5. AUTHENTIFICATION DES DONNEES

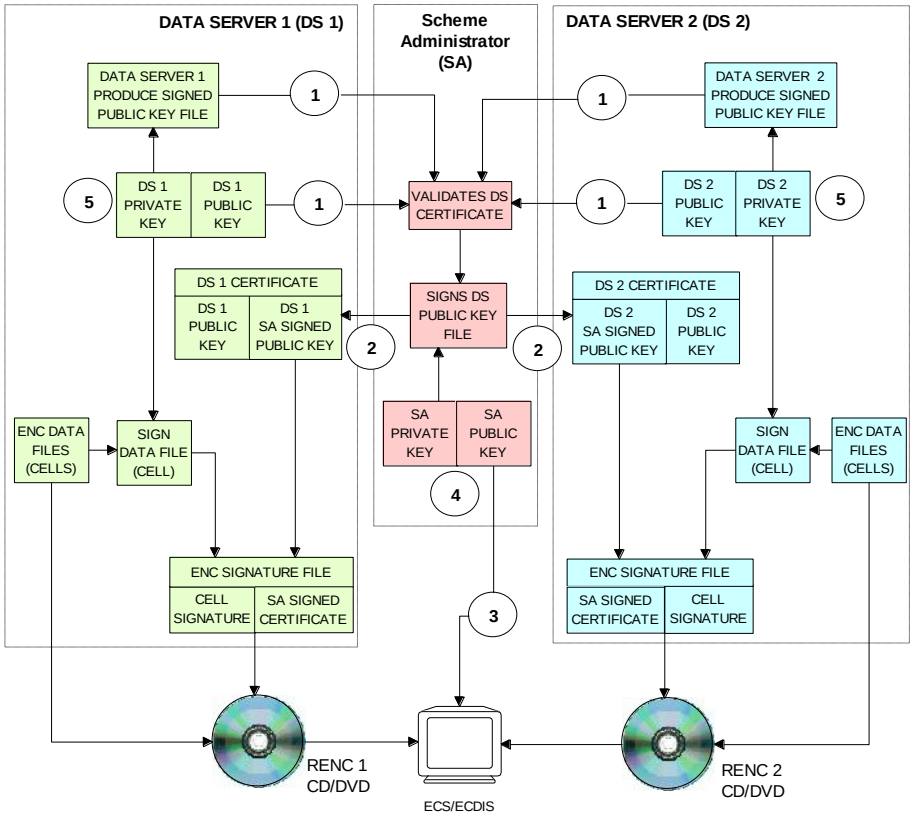
5.1 Introduction à l'authentification des données et au contrôle de l'intégrité

La technique de signature numérique utilisée dans le dispositif de la S-63 est basée sur un algorithme standard et un mécanisme d'échange de clés largement utilisé. Les signatures numériques de la S-63 utilisent des algorithmes asymétriques pour clés publiques au sein d'un dispositif d'infrastructure de type PKI pour lier de façon indéchiffrable un fichier de données à l'identité de l'éditeur.

Le dispositif est basé sur le chiffrement asymétrique[7] d'une somme de contrôle d'un fichier de données. En vérifiant la signature par rapport à la clé publique de l'éditeur, et également en vérifiant la clé publique de l'éditeur par rapport à une identité dite « top level », l'utilisateur s'assure de l'identité du signataire. Une explication détaillée des signatures numériques dépasse la portée de ce document et le lecteur doit se reporter à la publication FIPS 186 - Norme de signature numérique (www.itl.nist.gov/div897/pubs/fip186.htm) pour de plus amples et aisément accessibles explications.

On peut considérer que le dispositif comporte trois phases distinctes :

1. Un Administrateur du dispositif (SA) vérifie l'identité d'un fournisseur d'informations relatives aux ENC et lui fournit des données lui permettant de signer des données pour ENC.
2. Un Fournisseur de données (par exemple RENC ou VAR) émet des données ENC signées avec son identité (et sa vérification par le SA).
3. La vérification ultérieure par le client utilisateur de données de l'identité du fournisseur de données (dans le cadre de son association avec le SA) et de l'intégrité des données ENC.

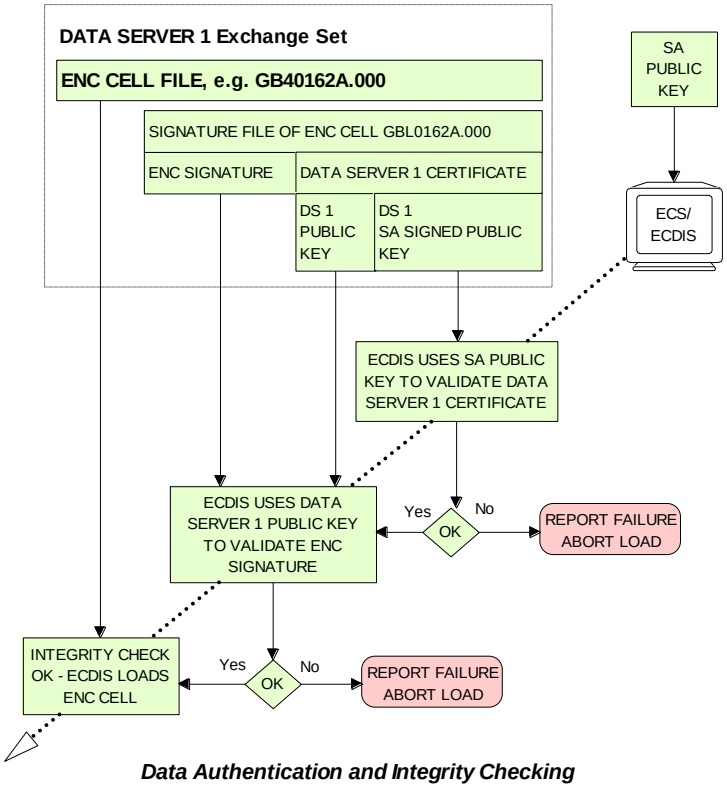


ENC AUTHENTICATION PROCESSES

[7] La cryptographie asymétrique est basée sur des algorithmes dans lesquels le chiffrement et le déchiffrement ont lieu au moyen de différentes clés cryptographiques. Toutefois, une personne peut chiffrer des données et mettre à disposition une clé de déchiffrement afin que d'autres puissent la déchiffrer. Il est fait référence à ces clés en tant que « clé privée » et « clé publique » collectivement appelée « paire de clés ».

NOTES – PROCESSUS D'AUTHENTIFICATION DES ENC

1. Les fichiers de clé publique et de clé auto-signée (SSK) du fournisseur de données sont envoyés au SA pour validation lorsque celui-ci demande à s'inscrire au dispositif de protection des données de l'OHI S-63.
2. S'ils sont acceptés, le SA signe le SSK du fournisseur de données avec sa propre clé privée pour produire un certificat de fournisseur de données signé par le SA, qui est ensuite renvoyé au fournisseur de données.
3. La clé publique de SA est distribuée largement et elle est installée indépendamment dans les systèmes des fabricants.
4. Les paires de clés publique et privée du SA doivent être différentes de tous les autres fournisseurs de données.
5. Toutes les clés publique et privée du fournisseur de données doivent être unique l'une par rapport à l'autre et par rapport au SA.



Data Authentication and Integrity Checking

NOTES – AUTHENTIFICATION DES DONNEES ET CONTROLE D'INTEGRITE

Si un ECS/ECDIS utilise la méthode décrite plus haut, et si la paire de clés du SA est différente de celle du fournisseur de données, il est alors capable d'authentifier et de valider les ENC à partir du fournisseur de données 2 (ou tout autre fourniseur de données dans le dispositif) en utilisant la même clé publique du SA.

1. **Authentification :** L' ECS/ECDIS utilise la clé publique de SA, précédemment installée indépendamment du CD-ROM, pour vérifier la partie certificat du fichier signature qui confirme que la clé publique du fournisseur dans le certificat est valide. C'est-à-dire que le fournisseur de données est un authentique membre du dispositif**.**

2. **Contrôle d'intégrité:** L'ECS/ECDIS utilise la clé publique du certificat pour contrôler la signature du fichier de (données) cellule ENC**.**

5.1.1 Vérification du SA

L'ECDIS doit pouvoir vérifier que les ENC proviennent d'une source authentique. Pour ce faire, il doit faire en sorte que les données de clé publique du fournisseur de données qui ont été fournies dans les fichiers de signature ENC soient validées par rapport à la clé publique du SA.

Le SA fournit des certificats à chacun des fournisseurs de données du dispositif ; chaque certificat est unique, le SA doit mener à bien cette tâche seulement une fois pour chaque fournisseur de données au moment où ce dernier rejoint le dispositif. Pour obtenir un certificat, les fournisseurs de données produisent une paire de clés et fournissent leurs clés publiques au SA (en tant que certificat auto-signé) ; le SA (à l'aide de la paire de clés existante) utilise sa clé privée pour signer la clé publique du fournisseur de données. Le certificat qui en résulte contient une signature de la clé publique du fournisseur. Ce certificat est ensuite inclus dans les fichiers de signatures des cellules et des mises à jour ENC.

Le SA diffuse largement sa clé publique auprès des utilisateurs d'ECDIS et les fabricants doivent fournir à l'utilisateur un moyen de la charger indépendamment des données.

5.1.2 Intégrité des données

Après que la source de l'ensemble d'échange ENC ait été authentifié, l'ECDIS contrôle l'intégrité des données en validant le fichier signature fourni pour chaque ENC par le fournisseur de données.

Le fournisseur de données crée pour chaque cellule un fichier signature qui comprend les deux parties suivantes :

La signature de l'ensemble de données [qui est créée à l'aide de la clé privée du fournisseur de données, de la moitié de la paire de clé du fournisseur de données (en substance la somme de contrôle chiffrée des données) et qui est différente pour chaque cellule].
Son certificat de fournisseur de données (qui demeure constant).

L'ECDIS utilise la clé publique du fournisseur de données qui est incluse dans le certificat pour valider la signature du fichier de données (il décode cette signature du fichier de données et compare la somme de contrôle avec la cellule ENC). Si ce contrôle de validation est couronné de succès alors cela prouve que les ENC n'ont pas été corrompues de quelque façon que ce soit et que l'identité du fournisseur de données est validée dans les signatures de cellule par le SA.

5.2 Certificats numériques (Authentification du SA)

Les certificats sont des fichiers numériques publiés par une autorité de certification. Ils lient une clé publique et d'autres informations à un particulier ou à une organisation. Les certificats contribuent à empêcher quelqu'un d'utiliser une fausse clé publique pour se faire passer pour quelqu'un d'autre. Le dispositif utilise une chaine de certificats, chacun certifie le précédent jusqu'à ce que toutes les parties soient assurées des indentités en question. Le certificat de SA utilisé par l'OHI sera un certificat[8] autosigné et est le certificat d'origine pour le dispositif.

Le SA publiera un certificat numérique pour l'ensemble des fournisseurs de données en signant le fichier de clé publique vérifiée du fournisseur de données. La liste des opérations dites «top level » réalisées lors de la publication des certificats numériques est donnée ci-dessous :

Création du dispositif

- Le SA crée une unique paire de clés dites « top level » publique et privée.

Etablissement d'un fournisseur de données

- Le fournisseur de données crée une unique paire de clés publique et privée.
- Le fournisseur de données crée une clé auto-signée (SSK) en signant son propre fichier de clé publique avec sa propre clé privée.
- Le fournisseur de données fournit la clé publique autosignée (SSK) au SA par un moyen fiable.
- Le SA vérifie la clé publique autosignée (SSK) du fournisseur de données en utilisant la clé publique du fournisseur de données.

[8] La clé publique du SA signée en utilisant la clé privée du SA.

- Le SA signe le fichier de clé publique vérifiée du fournisseur de données en utilisant la clé privée du SA.
- Le SA fournit au fournisseur de données son propre certificat unique de fournisseur de données signé par le SA.

Création d'ensembles de données signées

- Le fournisseur de données vérifie le certificat qui en résulte avec la clé publique du SA (fournie séparément).
- Le fournisseur de données conserve le certificat vérifié et l'utilise pour créer les fichiers de signature ENC.

Le format des différents fichiers, certificats et signatures est décrit plus en détails à la section 5.4.

NOTE: La clé publique du SA est diffusée largement à toutes les parties intéressées, par exemple les fournisseurs de données, les clients de données et les fabricants, par des moyens divers, comme le exemple web, courrier électronique, etc.

5.2.1 La clé publique du SA

Le dispositif demande que la clé publique de SA soit installée sur les systèmes des clients utilisateurs de données de l'ensemble d'échange ENC. Celle-ci peut être pré-installée par le fabricant. Cependant, le système du client utilisateur de données doit avoir une méthode pour installer une nouvelle clé publique[9] sur le système au cas où une nouvelle clé serait publiée par le SA.

L'utilisateur installe un nouveau certificat de SA ou clé publique et le système doit confirmer qu'il a bien été installé. Si un nouveau certificat de SA est installé (IHO.CRT) le système doit informer l'utilisateur de la manière suivante :

"Un nouveau certificat de SA (clé publique) a été installé qui est valide jusqu'au [entrer la date d'expiration] ou à moins que le SA n'en publie un nouveau pour des raisons de sécurité."

Si une nouvelle clé publique de SA est installée (IHO.PUB) le système doit informer l'utilisateur comme suit :

"Une nouvelle clé publique de SA a été installée qui est valide jusqu'à ce que le SA publie systématiquement une nouvelle clé publique ou à moins qu'une nouvelle clé ne soit publiée pour des raisons de sécurité. "

Si le système rapporte une erreur d'authentification au cours du processus de chargement, il doit alerter l'utilisateur de la possibilité que la clé publique ait été changée par le SA. Toutefois un message d'avertissement doit être affiché qui en explique la raison, comme suit:

"SSE 06 – Le certificat/clé publique de SA est invalide. Le SA peut avoir publié une nouvelle clé publique ou les ENC peuvent provenir d'un autre service. Une nouvelle clé publique de SA peut être obtenue à partir du site web de l'OHI ou auprès de votre distributeur. "

5.2.2 Nouveaux fournisseurs de données

L'OHI, en conjonction avec le DPSWG, établira l'identité de toute organisation ou société commerciale qui souhaite rejoindre le dispositif de protection, en tant que fournisseur de données. Si le certificat de fournisseur de données est annulé par le SA, elle informera du changement tous les fournisseurs de données et les fabricants.

[9] Il est prévu que les fournisseurs de données les fournissent indépendamment de l'ensemble d'échange afin qu'elles coïncident avec les données qui l'authentifient par rapport à la nouvelle clé publique.

5.3 Signatures numériques (Vérifier l'intégrité des données)

Une signature numérique est une signature électronique qui peut être utilisée pour authentifier l'identité de l'expéditeur d'un message ou le signataire d'un document, et pour s'assurer que le contenu original du message envoyé est inchangé. Les signatures numériques sont transportables, facilement vérifiables et ne peuvent être falsifiées. Il est également possible que les Services hydrographiques ou les autres organisations qui fournissent des données (par exemple RENC/VAR) utilisent les signatures digitales pour maintenir la provenance et l'intégrité des données entre eux au cours de la diffusion des informations ENC.

Chaque fichier ENC (les fichiers de base et les mises à jour) sera toujours associé à un seul fichier de signature unique. Aucun autre fichier d'un ensemble d'échange ENC chiffré ne possède de signature numérique.

NOTE: Un ensemble d'échange peut contenir des signatures publiées par différents fournisseurs de données et donc chaque dossier ENC doit être authentifié individuellement.

5.3.1 Vue d'ensemble au niveau technique des signatures numériques

L'authentification des données est obtenue en utilisant une signature numérique conforme à la Norme de signature numérique (DSS) [2]. La DSS utilise l'algorithme de hachage sécurisé (SHA-1) [3] pour créer un résumé de message (haché). Celui-ci est ensuite passé dans l'algorithme de signature numérique (DSA) [2] pour générer la signature numérique destinée au message en utilisant un algorithme de chiffrement asymétrique et la « clé privée » d'une paire de clés. Les algorithmes asymétriques ont la propriété que les données chiffrées utilisant la « clé privée » de la paire de clés ne peuvent être déchiffrées qu'en utilisant la « clé publique » de la paire de clés.

Une des conséquences du chiffrement du message traité avec la clé privée est que quiconque en possession de la clé publique (qui, comme son nom l'indique, peut être rendue publique) est capable de déchiffrer et de vérifier le résumé de message.

De plus amples informations sur les signatures numériques et leur utilisation peuvent être obtenues à partir du site web de l'OHI (http://www.iho.int).

5.3.2 Convention de dénomination du fichier de signature ENC

Le fichier de signature numérique correspondra au nom de fichier de cellule à l'exception des codes relatif à la navigation, chiffres de 1 à 6, qui seront remplacés par les caractères I à N.

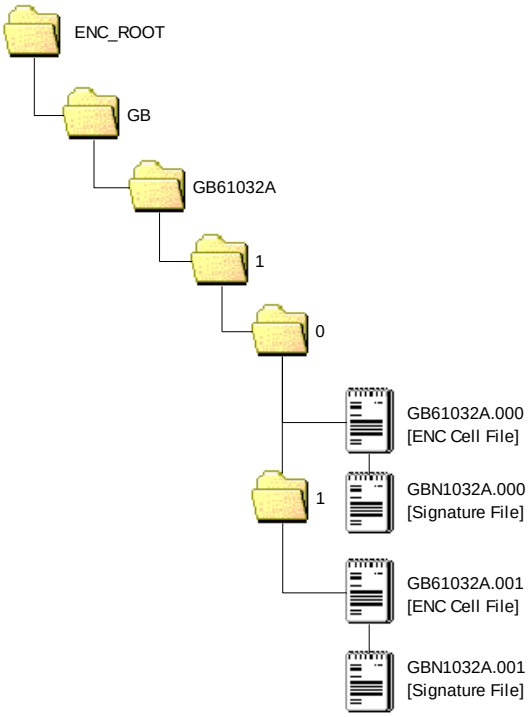
En général:
Fichier ENC : CC[1-6]XXXXX.EEE (voir l'Appendice B1 de la S-57)
Fichier de signature: CC[I-N]XXXXX.EEE

Type de navigation	**Caractère utilisé pour la signature**
1. Vue d'ensemble	I
2. Général	J
3. Côtier	K
4. Approches	L
5. Portuaire	M
6. Mouillage	N

Exemple:
Le fichier de cellule GB100001.000 possèdera un fichier de signature appelé GBI00001.000
Le fichier de cellule GB61032A.002 possèdera un fichier de signature appelé GBN1032A.002

5.3.3 Stockage du fichier de signature ENC

Le fichier de signature doit être identifiable de façon unique comme appartenant à un fichier particulier de données ENC ainsi qu'exposé dans la section 5.3.2 ci-dessus. Le fichier de signature numérique sera toujours localisé dans le même répertoire que le fichier de cellule ENC correspondant (voir ci-contre).



ENC DIGITAL SIGNATURE FILES PLACEMENT

5.4 Format de fichier d'authentification des données

Il existe de nombreux fichiers relatifs aux processus d'identification du Dispositif de protection des données de la S-63. Parmi eux, les fichiers de certificats et de signature tels que décrits dans les sections 5.2 & 5.3 et les clés privée/ publique créées pour les signer et les authentifier. Bien qu'elles puissent être obtenues indépendamment, les différentes composantes contenues dans chaque dossier ont des éléments communs qui sont toujours formatés de la même manière. Le tableau suivant liste les fichiers qui sont indispensables à l'authentification des ENC chiffrées selon la norme S-63. Ce tableau identifie également les participants au dispositif qui les ont créées

Types de fichier	Administrateur du dispositif	Fournisseur de données
Fichiers PQG	✓	✓
Clé privée (fichier X)	✓	✓
Clé publique (fichier Y)	✓	✓
Certificat X509 v3	✓	×
Clé auto-signée (SSK)	×	✓
Certificat	✓	×
Signature	×	✓

5.4.1 Eléments de fichier

Tous les éléments sont composés de deux parties, un en-tête et une chaîne de données. Le tableau suivant liste tous les éléments possibles qui peuvent convenir pour créer un fichier, un certificat ou une signature particulière.

Elément	En-Tête	Chaîne de données
R	// Signature part R:	10 blocks of 4 characters.
S	// Signature part S:	10 blocks of 4 characters.
p	// BIG p	32 blocks of 4 characters.
q	// BIG q	10 blocks of 4 characters.
g	// BIG g	32 blocks of 4 characters.
x	// BIG x	10 blocks of 4 characters.
y	// BIG y	32 blocks of 4 characters.

5.4.1.1 Formatage de l'en-tête des éléments et de la chaîne de données

Chaque chaîne de données :

- Est précédée d'une seule ligne en-tête. Les lignes en-tête sont signalées par deux barres obliques (// ASCII - 0x2F2F) au début suivies d'un espace (SP ASCII 0x20) et les caractères en tête sont en texte ASCII selon les descriptions de format ci-dessous :
- Est exprimée en hexadécimales et ASCCII (0-9, A-F). Tout caractère alphabétique sera en majuscules.
- Se termine par un point (. ASCII 0x2E).

- A un espace de séparation entre chaque groupe de 4 caractères (ASCII SP 0x20).
- A un délimiteur fin de ligne (ASCII CR 0x0D) et une nouvelle ligne (ASCII LF 0x0A) à la fin de chaque chaîne de données. Has a Carriage Return (ASCII CR 0x0D) and New Line (ASCII LF 0x0A) at the end of each data string.

5.4.2 Exemples de formats de fichier, de certificat et de signature

La section suivante comprend un ensemble d'exemples de tous les différents dossiers liés à cet aspect du dispositif de protection des données de la S-63. Une explication détaillée de la manière dont ces fichiers sont créés est précisée plus loin dans ce document.

5.4.2.1 Format PQG

Les paramètres PQG sont produits à partir d'une chaîne aléatoire et utilisés pour créer les paires de clés publique/privée X et Y. Après que celles-ci aient été réalisées, on trouvera les paramètres PQG dans les paires de clé privée/publique X et Y

P, Q et G sont les paramètres numériques utilisés dans l'algorithme de signature numérique en tant qu'entrée dans le processus de création de clés. Chaque fournisseur de données peut utiliser un ensemble différent P, Q et G ou utiliser un ensemble existant pour générer des paires de clés aléatoires. La norme de signature numérique [2] décrit leur origine et leur utilisation.

Exemple de format PQG :

```
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
```

5.4.2.2 Le format X (clé privée)

Le fichier X doit être écrit en langage ASCII dans le format suivant:

```
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG x
EBAF 2948 1485 7E7C 2F48 C7B2 9334 2F09 DA1A EB04.
```

5.4.2.3 Le format Y (clé publique du fournisseur de données ou de l'OHI)

La clé publique du SA et celle du fournisseur de données sont fournies dans le format suivant, le dispositif utilisant une clé publique DSA d'une longueur de 512 bits.

```
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.
```

5.4.2.4 Le format de certificat numérique du SA (X509v3)

Le certificat numérique du SA sera au format X509v3 [4] et représentera la clé publique DSA d'une longueur de 512 bits. Le certificat numérique de SA sera disponible dans un fichier appelé IHO.CRT. Le fichier IHO.CRT est disponible sur le site web de l'OHI : http://www.iho.int.

Tous les fournisseurs de données assurant un service ENC peuvent inclure le certificat de SA, comme référence dans le répertoire racine du média (c'est-à-dire D:\IHO.CRT on a CD-ROM) mais, comme Indiqué dans la section 5.2.1, l'installation sur un système de client utilisateur de données du certificat SA doit être faite indépendamment. Le contrôle de validité de la signature du SA à l'intérieur de chaque fichier signature ENC doit être fait à partir de la version du certificat de SA installée indépendamment.

La clé publique du SA au format ASCII (par opposition au format binaire X509v3) est également disponible sur le site web de l'OHI à http://www.iho.int (le format est décrit à la section 5.4.2.3).

5.4.2.5 Le format de clé auto-signée (SSK)

Il s'agit du format de fichier que le fournisseur de données utilise pour signer sa propre clé publique avant de l'envoyer au SA pour signature. La signature est la signature du fichier de clé publique complet (c'est-à-dire le PQG et les paramètres Y).

```
// Signature part R:
752A 8E5C 3AF5 6CCD 7395 B52E F672 E404 554F AAB6.
// Signature part S:
1756 E5C0 F4B6 BC90 4EC6 5F94 DF93 3ADF 68B8 86C4.
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.
```

Single Signature Element
Data Server (DS) Signature of DS Public Key

Data Server Public Key

Data Server Public Key File

The DS Signature is authenticated by the SA against the DS supplied Public Key

5.4.2.6 Format de fichier de certificat de fournisseur de données signé par le SA

Il s'agit du format de fichier utilisé par le SA lorsqu'il publie un fichier de certificat de fournisseur de données. Le SA utilise également la clé publique DSA d'une longueur de 512 bits. La paire « R & S » constitue ce qui est transcrit dans les fichiers signature ENC du fournisseur de donnée**.**

```
// Signature part R:
8FD6 2AC7 27D2 8D0B CD27 BDF2 5CC6 9656 10E3 751F.
// Signature part S:
3DE7 DA37 5A40 80FC 4203 5C6E 37DE A984 2A88 2BDC.
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.
```

Single Signature Element
SA Signature of DS Public Key

Data Server Public Key

Data Server Public Key File

SA Signed Data Server Certificate

The SA Signature is authenticated by the SA Public Key held in the ECS/ECDIS

5.4.2.7 Le format de fichier de signature pour ENC

Le fichier de signature doit contenir une signature et un certificat. Un fichier comprenant une seule signature n'est pas valide car il ne certifie pas l'identité du fournisseur de données. Le format, la structure et l'ordre du fichier de signature numérique pour ENC est tel que dans l'exemple suivant :

```
// Signature part R:
77D3 4D86 DA6E 6E01 7058 7140 74FC 7E3D 21CD E80B.
// Signature part S:
04A1 7B52 081F B6CE 10FE 5AD9 1CCE 3F25 FEAC DA05.
// Signature part R:
8FD6 2AC7 27D2 8D0B CD27 BDF2 5CC6 9656 10E3 751F.
// Signature part S:
3DE7 DA37 5A40 80FC 4203 5C6E 37DE A984 2A88 2BDC.
// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.
```

First Signature Element
Data Server Signature of ENC Data File

Second Signature Element
SA Signature of the Data Server Certificate

Data Server Public Key

Data Server Public Key File

SA Signed Data Server Certificate

The first Signature/R & S Pair is authenticated by the Data Server's Public Key

The second Signature/R & S Pair is authenticated by the SA Public Key stored in the ECS/ECDIS

La seconde paire R et S est utilisée pour authentifier le certificat numérique de fournisseur de données (chaînes p, q, g et y). Si elle est vérifiée avec succès, la clé publique de fournisseur de données (chaîne y) peut être extraite et utilisée pour vérifier la signature numérique (première paire « R & S ») de l'ENC chiffrée. Ceci permet au client utilisateur de données de vérifier le certificat numérique du SA, pour extraire la clé publique du fournisseur de données et de vérifier la signature numérique des données ENC.

Page laissée en blanc intentionnellement

6. GESTION DES DONNEES

6.1 Introduction

Le chargement et l'importation des ENC vers un ECS/ECDIS doivent être gérés avec soin; ceci est particulièrement vrai dans un environnement de fournisseurs de données multiples. Etant donné que le dispositif chiffre le contenu complet d'un fichier de cellule ENC (base et mise à jour), ceci réduit l'accès à certains sous-champs dans un fichier de cellule ENC exigés par les systèmes de fabricants pour gérer l'importation des ENC vers le SENC ECS/ECDIS. En conséquence des fichiers additionnels de la S-63 sont nécessaires pour compléter ces données inaccessibles ainsi que comme modification d'un fichier S-57 existant, par exemple le fichier CATALOG.031.

On a également noté que l'importation de nombreuses ENC a rendu certains aspects de la S-57 peu pratiques à implémenter, par exemple un unique ensemble de données d'échange se répartit en volumes pour média multiples. Pour cette raison, il est devenu nécessaire de modifier la stratégie de chargement et d'utiliser les fichiers additionnels de la S-63 pour mieux gérer l'installation et le chargement des ENC dans des ensembles multiples de données d'échange.

Comme indiqué précédemment, la S-63 est destinée à fonctionner dans un environnement de fournisseurs de données multiples. La S-57 ne possède pas de mécanisme permettant de différencier les ensembles de données d'échange pour ENC mis à disposition par les différents fournisseurs de données et il a donc été nécessaire d'en produire un dans la version 1.1 de cette norme.

Les fichiers additionnels de la S-63 contiennent des renseignements importants qui, utilisés correctement, peuvent rendre plus efficace et intuitif le processus d'importation de la S-57 pour le client utilisateur de données. Ces renseignements sont détaillés plus avant dans cette section.

La méthode de chargement/importation peut être décomposée dans les différents processus suivants:

- Gérer l'importation des ensembles de données d'échange spécifiques du fournisseur de données en utilisant l'identification du fournisseur de données.
- Gérer le service du fournisseur de données s'il est étendu sur de multiples ensembles de données d'échange.
- Gérer l'importation des cellules ENC ayant reçu la licence de manière consécutive, en faisant en sorte que toutes les cellules ENC de base et les fichiers de mises à jour correspondants, soient importés correctement et de manière séquentielle.
- Gérer l'importation de fichiers texte et image en maintenant une relation entre ces derniers et le fichier de cellule auquel ils sont associés..

La table suivante liste les fichiers additionnels de la S-63 et les modifications de fichiers ainsi que leur principales raison d'être dans la S-63. Ces fichiers et leurs formats associés sont détaillés plus avant aux sections 6.2, 6.3 et 6.4.

Fichier/Champ	Fonction de gestion primaire
PRODUCTS.TXT	Il est nécessaire de fournir les informations suivantes : La date de publication du fichier 'produits' installé. Un catalogue de l'ensemble des cellules disponibles dans un service de fournisseur de données. La couverture de l'ensemble des cellules dans un service. La date de publication la plus récente, pour toutes les cellules disponibles dans un service (y compris les cellules annulées). L'ensemble de données d'échange destinataire (base ou mise à jour) où réside le fichier de cellule ENC de base (profil d'application EN). Ceci peut être une cellule de base, une nouvelle édition ou une réédition.
SERIAL.ENC	Il est nécessaire de fournir les informations suivantes : L'identification du fournisseur de données. Le numéro hebdomadaire et la date de publication de l'ensemble de données d'échange. Le type de l'ensemble de données d'échange (base ou mise à jour). Le numéro de l'ensemble de données d'échange dans une série multiple.
CATALOG.031 [CATD-COMT]	Il est nécessaire de fournir les informations contenues à l'origine dans le champ DSID du fichier de cellule, pour importer le contenu complet et séquentiel d'un ensemble de données d'échange.

6.2 Listage de produits ENC (PRODUCTS.TXT)

Le fichier intitulé 'PRODUCTS.TXT' sera fourni avec chaque ensemble de données d'échange chiffré et stocké dans un dossier dénommé « INFO » conservé dans le répertoire principal. Il contient le mécanisme de gestion des données au sein d'un service ENC et d'échange de ces données avec celles déjà contenues dans le SENC du client utilisateur de données. La structure et le format de ce fichier est décrit avec plus de détails dans les sections 6.2.1, 6.2.2, 6.2.3 et 6.2.4.

Il y a deux types de fichier PRODUCTS.TXT, "PARTIEL" et "COMPLET". Un listage de produits partiel comprend l'état actuel de toutes les ENC contenues dans un seul ensemble de données d'échange. Un listage de produits complet comprend l'état actuel de TOUTES les cellules contenues dans un service de fournisseur de données, c'est-à-dire, tous les ensembles de données d'échange. Bien que les procédures puissent varier entre fournisseurs de données un listage de produits complet sera toujours fourni avec l'ensemble de données d'échange mis à jour sur une base hebdomadaire. Dans les cas où un fournisseur de données publie un ensemble complet de nouveaux supports de base (pas de mise à jour hebdomadaire), chacun d'eux doit contenir un listage de produits complet de toutes les ENC dans un service.

NOTE: Les fabricants doivent faire en sorte que leurs systèmes soient capables d'intégrer les listages de produits "COMPLET" et "PARTIEL" (voir section 6.2.2). Les CD-ROM de base peuvent contenir un listage partiel ne comprenant que la table des matières du CD-ROM inclus. La mise à jour comportera toujours un listage de produit complet des ENC disponibles dans un service de fournisseur de données.

La licence et les informations relatives aux ENC provenant de différents fournisseurs de données doivent être stockées indépendamment sur le système du fabricant. Le fichier SERIAL.ENC (voir section 6.3) contient l'indentification du fournisseur de données et doit être utilisé en conjonction avec le listage de produits associé afin d'identifier la source du service. Le dernier listage de produits conmprend l'état actuel des données des cellules ENC dans un service. Ce fichier est utilisé pour comparer les données des cellules ENC disponibles dans un ensemble de données d'échange avec les informations déjà stockées dans les SENC des fabricants. Le système du fabricant peut donc définir les nouvelles données disponibles pour importation.

Il est recommandé que les fabricants conservent une copie des derniers listages de produits sur leurs systèmes ce qui reflétera l'état actuel d'un service en particulier. Pour gérer à la fois les listages de produits «COMPLETS" et "PARTIELS", il est primordial que les nouvelles informations fusionnent avec les données existantes stockées et qu'elles ne soient pas recouvertes.

6.2.1 Structure de fichier de listage de produit

Le contenu du listage de produits sera divisé en deux sections. Le fichier de liste de produits est entièrement codé en langage ASCII et comprend trois sections, à savoir :

Section	Description
En-tête	Comprend les informations générales sur la nature de la liste de produits, par exemple, la date de création ou le numéro de version.
:ENC	Comprend l'état actuel de toutes les cellules/mises à jour ENC fournies par le fournisseur de données
:ECS	Comprend les informations relatives aux autres informations cartographiques numériques fournies par le fournisseur de données.

6.2.2 En-tête de la liste de produits

La liste de produits commence avec une section en-tête. La section en-tête est composée de plusieurs enregistrements. Chaque enregistrement commence à une nouvelle ligne et se termine avec les caractères ASCII CR/LF comme dans les fichiers de signature.

L'en-tête est composé des champs de renseignements tels que définis dans l'exemple et le tableau ci-dessous. Tous les champs sont obligatoires et sont toujours définis dans le même ordre.

Champs	Nom du champ	Valeur
Date et heure	**:DATE**	`YYYYMMDD HH:MM` Le nom du champ, la date et l'heure sont séparés par un caractère <espace>. La date est donnée sous la forme 20060627 et l'heure sous la forme 09:00:00 en utilisant le cadran de 24 heures. Exemple : `DATE 20061019 09:00:00`
Version de la liste de produits	**:VERSION**	Nombre entier de 1 à 99 Il sera augmenté de 1 à chaque nouvelle version de la spécification du fichier PRODUCTS.TXT. L'édition 1.1 de la S-63 définit la valeur comme étant «2 ». Par exemple : `VERSION 2`
Contenu	**:CONTENT**	"`COMPLET`" Copie complète de la liste de produits "`PARTIEL`" Copie complète de la liste de produits Code utilisé pour indiquer si le fichier de la liste de produits une copie complète ou partielle de la liste de produits complète. Exemple: `CONTENT FULL`

Exemple:

```
:DATE 20061019 09:00:00
 :VERSION 1
 :CONTENU COMPLET
```

6.2.3 Section "ENC" de la liste de produits

La liste de produits contient toujours une section ENC. Elle contient des renseignements sur l'état actuel en matière de navigation de toutes les cellules et mises à jour officielles appuyées par le fournisseur de données.

Cette section commence par un enregistrement de l'identificateur de section ENC tel que défini ci-dessous.

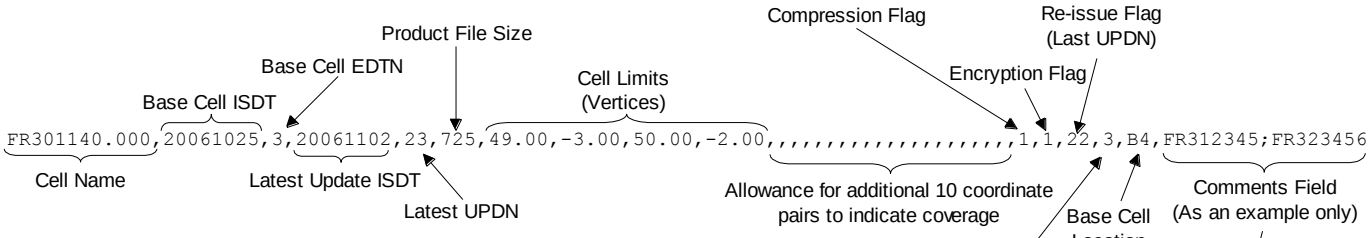
Champ	Nom du champ	Valeur
Identificateur de la section ENC	:ENC	Pas applicable

La section ENC se compose ensuite d'enregistrements répétitifs qui définissent l'état de chaque ENC distribuée par le fournisseur de données. La définition de cet enregistrement est détaillée dans la table ci-dessous :

Champ	Valeur
Nom du produit	Nom du produit tel que défini dans le sous-champ DSID-DSNM de l'édition 3 de la S-57. L'extension de fichier est toujours 000. Exemple: GB202400.000
Date de publication de la cellule de base	AAAAMMJJ Cette date est utilisée seulement pour les fichiers de cellules de base (par exemple, les nouveaux ensembles de données, les réimpressions et les nouvelles éditions) et non les fichiers de mise à jour. Toutes les mises à jour en date de ce jour ou avant doivent avoir été appliquées par le fabricant. Les cellules annulées avec le numéro d'édition '0' (zéro) portent la date de publication de la mise à jour utilisée pour l'annuler. Exemple: 20050222
Edition de cellule de base	Numéro d'édition de la cellule de base [EN] ENC. Nombre entier de 1 à 999 Identique au contenu DSID-EDTN de l'édition 3 de la S-57. Au cas où une cellule est annulée l'édition de produit est mise à « 0 » (zéro), voir section 6.2.3.1. Ceci permet au système ECDIS d'identifier rapidement les cellules qui ont été supprimées d'un service.
Date de publication de la dernière mise à jour [Profil d'application ER]	AAAAMMJJ Date à laquelle la dernière mise à jour relative à l'édition actuelle de la cellule ENC est publiée.On utilise ce champ dans tous les cas de mise à jour ou de ré-édition de cellule.
Numéro de la dernière mise à jour	Nombre entier de 1 à 999 Le numéro de mise à jour du dernier message de mise à jour publié pour l'édition de cellule ENC. Identique au contenu DSID-UPDN. En blanc lorsqu'aucune mise à jour n'est disponible en ce qui concerne l'actuelle édition de la cellule de base. Utilisé seulement pour les mises à jour et les publications.
Taille de fichier	Nombre entier de 1 à 999999 Taille totale du fichier en kilo-octets de tous les fichiers publiés sur le produit. Elle inclut la taille de la cellule de base, des mises à jour et de tout fichier texte et images applicable.
Latitude la plus au sud de la limite de cellule	Degrés d'arc, le sud est négatif. Latitude la plus au sud de la couverture de données du produit ENC. Exemple: 49.898773299986 (49°53´.93N)
Longitude la plus à l'ouest de la limite de cellule	Degrés d'arc, l'ouest est négatif. Longitude la plus à l'ouest de la couverture de données du produit ENC. Exemple: -1.927277300003 (001°55´.64W)
Latitude la plus au nord de la limite de cellule	Degrés d'arc, le sud est négatif. Latitude la plus au nord de la couverture de données du produit ENC. Exemple: 50.922828000014 (50°55´.37N)
Longitude la plus à l'est de la limite de cellule	Degrés d'arc, l'ouest est négatif. Longitude la plus à l'est de la couverture de données du produit ENC. Exemple: -0.000166700008 (000°00´.01W)
10 coordonnées de la couverture de données	Optionnel. Degrés d'arc, le sud et l'ouest sont négatifs. 10 paires de coordonnées peuvent être fournies pour indiquer la couverture de données de la cellule ENC. Ceci sera assuré par la répétition des paires de coordonnées Y et de coordonnées X.
Compression	Nombre entier de 0 à 99 "0" Pas de compression "1" Utilisation de la compression (voir section 2)

Champ	Valeur
Chiffrement	Nombre entier de 0 à 99 "0" Pas de chiffrement "1" Utilisation du chiffrement (voir section 3)
Numéro de mise à jour de la cellule de base	Si une cellule est ré-éditée, le numéro de la mise à jour en vigueur à la date de la ré-édition devrait être inséré ici. Si une édition de cellule n'est pas ré-éditée alors ce champ est blanc ou rempli de zéros.
Dernier numéro de mise à jour de l'édition précédente	Vide si aucune édition précédente n'est disponible dans la base de données du fournisseur de données. Si les précédentes éditions de la cellule sont disponibles alors ce champ renfermera le dernier numéro de mise à jour de l'édition précédente.
Localisation de la cellule de base	**CD-ROM** Position au sein de l'ensemble de données d'échange où l'on peut trouver la cellule de base. Les cellules de base peuvent être situées sur un ou plusieurs ensembles de données d'échange de base ou de mise à jour. C'est un nombre entier de 1 à 99 suivi d'un "B" s'elle se trouve sur un CD-ROM de base ou de "U" si elle se trouve sur la mise à jour, par exemple : **B7, B11, U1**, etc. **Support à grande capacité** Au cas où un service appuie des médias de grande capacité, ce champ est divisé en deux sous-champs délimités par un « ; » (point virgule) Le premier sous-champ contient le numéro d'identificateur et le second le numéro d'ensemble de données d'échange. L'identificateur des médias est désigné par un **"M"** suivi d'un nombre. Par exemple, le numéro ExSet est formaté de la même manière que les CD-ROM, par **"B1".** Par exemple une cellule de base pourrait être localisée comme suit **"M1;B1", "M1;B2", "M2;B10**, etc. Les mises à jour par exemple "M1;U1" ou **M1;U2,** si plus d'une mise à jour ExSET se trouve sur le même média. Voir **Appendice 2** de ce document pour plus de détails.
Remplacements des cellules supprimées (Champ des commentaires périmés)	Si une cellule est supprimée et une (des) cellule (s) de remplacement est (sont) publiée(s), ce champ est utilisé afin d'identifier les remplacements. Au cas où il y a plus d'un remplacement, les noms de cellule seront délimités par un ";" (point virgule). Voir section 6.2.3.3 pour plus amples détails.

Exemple de structure et format :




```
:DATE 20061213 09:22
:VERSION 1
:CONTENT FULL
:ENC
FR301130.000,20020316,2,20061124,2,21,50.0,-3.0,51.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,0,2,B4,
FR301140.000,20061025,3,20061102,23,725,49.0,-3.0,50.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,22,3,B4,FR312345;FR323456
FR301150.000,20030412,3,20061124,26,744,48.0,-3.0,49.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,0,8,B4,
FR301160.000,20020413,2,20051206,13,87,49.0,-4.0,50.0,-3.0,,,,,,,,,,,,,,,,,,,,,1,1,0,5,B4,
FR301170.000,20020803,2,20061003,12,502,48.0,-4.0,49.0,-3.0,,,,,,,,,,,,,,,,,,,,,1,1,0,3,B4,
FR301180.000,20030830,3,20061114,1,34,49.0,-5.0,50.0,-4.0,,,,,,,,,,,,,,,,,,,,,1,1,0,3,B4,
```

6.2.3.1 Gestion des cellules annulées (Fournisseurs de données)

Lorsqu'une cellule est annulée par un SH, un fichier de cellule de mise à jour est créé, qui comprend seulement l'enregistrement des informations générales de l'ensemble de données avec le champ « Identificateur de l'ensemble de données » [DSID]. Le sous-champ « Numéro d'édition » [EDTN] du champ DSID doit être mis à 0 (zéro). Les messages d'annulation sont utilisés seulement pour annuler un fichier de cellules de base.

Dans un service chiffré, cette information n'est pas mise à disposition du client utilisateur de données à moins que la mise à jour ne soit d'abord déchiffrée. Pour éviter d'avoir d'abord à déchiffrer, il existe deux méthodes pour coder cette information dans un échange de données chiffrées à savoir :

1. Les sous-champs EDTN du champ CATD-COMT dans le fichier CATOLOG.031 (voir 6.4.1.1).
2. Le champ 'Edition de cellule de base' dans le fichier PRODUCTS.TXT (voir section 6.2.3).

Le fichier CATALOG.031 peut être utilisé pour identifier toute cellules annulée dans un ensemble de données d'échange à l'importation tandis que le fichier PRODUCTS.TXT sert à souligner toutes les cellules annulées dans un service de fournisseur de données. Les ENC qui ont été annulées doivent demeurer sur le média de base ou de mise à jour, avec les références du fichier PRODUCTS.TXT, pendant une durée minimum de 12 mois.

6.2.3.2 Gestion des cellules annulées (Clients utilisateurs de données)

Les cellules annulées sont les ENC qui ont été supprimées du service ENC d'un fournisseur de ddonnées et, en tant que telles, elles ne sont plus soutenues ou mises à jour par l'autorité éditrice. Il existe deux options pour les fabricants qui gèrent les cellules annulées, à savoir :

1. Supprimer automatiquement la cellule d'un SENC lorsqu'une cellule est identifiée comme étant annulée.
2. Permettre à l'utilisateur de décider de conserver ou d'enlever la cellule du SENC.

Les fabricants d'ECDIS/ECS peuvent décider de l'option qu'ils souhaitent implémenter dans leurs systèmes. Toutefois, il est important que le système informe l'utilisateur qu'une cellule spécifique est annulée et, dans le cas de l'option 2, des conséquences que le fait de la conserver pourraient entraîner.

En ce qui concerne l'option 1, l'utilisateur doit être informé qu'une cellule spécifique est annulée soit lors de la période de chargement, soit, de préférence, par un rapport à la fin du processus.

En ce qui concerne l'option 2, l'utilisateur a le choix de conserver ou d'enlever la cellule du SENC. Si l'utilisateur choisit de conserver la cellule un avertissement permanent doit être affiché sur l'écran, lorsque la cellule annulée est visualisée. Ce message doit être semblable à l'exemple ci-dessous.

"Cellule <nom> a été annulée et n'est peut-être pas à jour. Elle ne doit en aucun cas être utilisée pour la navigation principale".

6.2.3.3 Remplacement des cellules ENC annulées

Lorsqu'une cellule ENC a été annulée, elle est souvent remplacée par une ou plusieurs cellules ENC. Ceci peut être dû à une re-disposition de la part du fournisseur de données. Des dispositions ont été prises dans cette édition de la S-63 pour que cette information soit affichée dans le système du client utilisateur de données. Le champ des commentaires du fichier PRODUCTS.TXT est maintenant disponible pour l'affichage des informations relatives aux cellules remplacées. Le formatage de l'enregistrement de la cellule dans le listage des produits est indiqué à la section 6.2.3.

Lorsqu'une cellule est identifiée comme étant annulée, le client utilisateur de données doit lire le champ "Remplacement des cellules ENC annulées" pour vérifier si une (des) cellule (s) ENC

remplacée (s) a (ont) été codée (s). S'il en existe, le client utilisateur de données doit en informer l'utilisateur. Un message semblable à celui indiqué ci-dessous doit être affiché :
"Cellule <nom> a été annulée et remplacée par cellule (s) <nom1>; <nom2>. Veuillez prendre contact avec votre fournisseur de données pour obtenir les permis ENC additionnels ".

6.2.4 Section liste de produits 'ECS'

Le fournisseur de données peut également publier d'autres types de produits cartographiques numériques tels que les cartes d'arrière-plan qui peuvent être utilisées pour afficher la couverture cartographique. Les informations sur ces produits peuvent également être mises à disposition dans la liste de produits si le fournisseur de données le souhaite.

Le contenu de cette section est identique à la section ENC définie en 6.2.3. La seule différence est l'identificateur de Section qui sera : ":ECS".

Exemple de codage d'une liste de produits qui utilise tous les éléments définis à la section 6.2.1.

```
:DATE 20061019 09:00:00
:VERSION 1
:CONTENT FULL
:ENC
AR201130.000,20051118,1,20060703,1,,-36.43335487,-57.41667361,-34.69998565,-54.33335853,,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR302120.000,20051219,1,20060427,2,,-39.44997766,-62.39166614,-38.74168723,-61.11683505,,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402490.000,20051206,1,20060330,1,,-39.11668811,-61.94017540,-38.95167627,-61.76656919,,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402550.000,20051219,1,20060427,1,,-39.01664968,-62.16649373,-38.88332240,-61.94017540,,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402560.000,20051122,1,20060427,1,,-38.99166872,-62.39166614,-38.74168723,-62.16649373,,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR420010.000,20060912,2,,,,-35.16832135,-56.07497834,-35.03499407,-55.84166992,,,,,,,,,,,,,,,,,,,,,1,1,0,3,B3,
:ECS
PM1WORLD.000,19990101,1,,,3000,-90,-180.0,90.0,180.0,-90.0,-180.0,90.0,180.0,,,,,,,,,,,,,,,,,,,,0,0,,,B5,
```

6.3 Fichier en série (SERIAL.ENC)

Un fichier nommé SERIAL.ENC est fourni de façon à ce que les clients utilisateurs de données puissent identifier les informations suivantes avant de les importer:

- Identificateur du fournisseur de données (enregistré auprès du SA)
- Semaine de publication
- Date de publication
- Type de CD-ROM (Base ou mise à jour)
- Version du format
- Numéro d'ensemble d'échange de données (d'une série d'ensemble d'échange de données)

6.3.1 Format du fichier SERIAL.ENC

Le fichier SERIAL.ENC est fourni dans le but d'aider les systèmes du client utilisateur de données à gérer l'importation des CD-ROM d'ENC fournis par des fournisseurs de données spécifiques parmi de multiples ensembles de données d'échange. Il doit être le premier fichier de l'ensemble de données qui soit lu car il contient d'importantes informations concernant l'identificateur du fournisseur de données assigné par l'OHI, la date de publication du CD-ROM, le type de CD-ROM, le numéro de CD-ROM dans ce service de fournisseur de données particulier, etc.

Les contenus de ce fichier peuvent être retournés aux permis installés pour contrôler l'état de l'inscription du client utilisateur de données.

Champ identificateur	Domaine	Octets	Portée	Notes (voir ci-dessous)
Identificateur du fournisseur de données	caractère	2	Tout chiffre alphanumérique	1
Semaine de publication	caractère	10	Tout caractère ASCII	2
Date de publication	date	8	YYYYMMDD	3
Type de CD-ROM	Caractère	10	BASE ou MISE A JOUR	4

Champ identificateur	Domaine	Octets	Portée	Notes (voir ci-dessous)
Version du format	décimal	5	01.00 – 99.99	5
Numéro d'ensemble d'échange de données	caractère	6	B01-99X01-99 ou U01-99X01-99	6
Délimiteur de fin d'enregistrement	Caractère hexadécimal	3	0x0B0D0A	7

Notes	Explication et description
1	L'identificateur du fournisseur de données doit être enregistré auprès de l'OHI; lorsque le fournisseur de données est également un service hydrographique, le code agence de l'Organisation est tiré de la S-62 – Codes de l'OHI pour les agences productrices de données.
2	La semaine de publication indique la semaine et l'année auxquelles le CD-ROM est distribué, par exemple `WK12-99, WK45-99, WK23-00,` etc.
3	La date de publication est indiquée au format habituel de date `YYYYMMDD`, par exemple, `19990414, 20000102, 20061102`, etc.
4	Le CD-ROM peut être publié en deux différents types : BASE: Le format doit être défini comme étant le format BASE ; le CD-ROM contient toutes les EN et toutes les ER additionnelles. MISE A JOUR: Le format doit être défini comme étant le format MISE A JOUR; le CD-ROM contient toutes les nouvelles EN et toutes les ER publiées depuis la publication du dernier CD-ROM de base approprié.
5	La version du format décrit la version du fichier SERIAL.ENC. La version qui est rattachée à l'édition 1.1 de la S-63 est **02.00**
6	Ce champ doit être utilisé pour montrer le numéro de série de l'ensemble d'échange de données, par exemple `B02X03`, qui égale le CD-ROM de base No. 2 sur un total de 3 CD-ROM de base `U01X01` qui égale le CD-ROM 1 de mise à jour sur un total de 1.
7	La fin du délimiteur de fin d'enregistrement est composé de caractères binaires, et il faut donc faire atttention lorsqu'on essaie d'éditer le fichier – il ne peut pas être édité en Windows Notepad! C'est la raison pour laquelle le fichier SERIAL.ENC doit toujours être édité en langage ASCII/Hexadécimal. Le délimiteur n'a normalement pas besoin d'être changé. Le délimiteur utilisé est `0x0B0D0A`.

Le fichier SERIAL.ENC doit être stocké directement sous le fichier principal du média, c'est à dire au même niveau que les répertoires ENC ROOT et INFO.

Exemple de fichiers SERIAL.ENC

```
PRWK15-99    19990414BASE       02.00B02X030x0B0D0A
PRWK20-99    19990601UPDATE     02.00U01X010x0B0D0A
```

(Où `0x0B0D0A` représente la fin du délimiteur d'enregistrement converti en chiffres hexadécimaux).

6.4 Le fichier du catalogue de la S-57 (CATALOG.031)

Le champ "Identification de l'ensemble de données" [DSID] est utilisé par l'ECS/ECDIS pour permettre d'importer les cellules de base et les fichiers de mise à jour vers le SENC de façon séquentielle et sans omission. Etant donné que le fichier complet de cellule ENC est chiffré, les informations du champ DSID de chaque fichier de cellule ne sont pas disponibles pour les systèmes fabricants, à moins d'être d'abord déchiffrées.

Le champ "Commentaires" [CATD-COMT] de chaque enregistrement de cellule du fichier CATALOG.031 est utilisé pour stocker les informations DSID exigées. Etant donné que le fichier CATALOG.031 tient lieu de table des matières pour l'ensemble des données d'échange et détermine où les fichiers sont stockés, il est tout à fait désigné pour remplir ce rôle.

Les informations stockées dans ce champ doivent être identiques à celles stockées dans le champ DSID qui quant à elles doivent correspondre à la section 5.7 de l'appendice A – Spécification de produit - de la S-57 de l'OHI. Ceci est résumé dans le tableau ci-dessous, qui spécifie les règles de codage des profils d'application EN et ER des ENC.

Evènement	Extension du fichier	EDTN	UPDN	UADT	ISDT	Commentaires
Nouvelle cellule ENC	.000	1	0	19950104	19950104	UADT< ou = ISDT
Mise à jour 1	.001	1	1	Annulée	19950121	ISDT seulement
Mise à jour 2	.002	1	2	Annulée	19950225	ISDT seulement
...						
Mise à jour 31	.031	1	31	Annulée	19950905	ISDT seulement
Réédition d'une cellule ENC	.000	1	31	19950905	19950910	UADT < ou = ISDT
Mise à jour 32	.032	1	32	Annulée	19951023	ISDT seulement
...						
Mise à jour 45	.045	1	45	Annulée	19951112	ISDT seulement
Nouvelle édition de cellule ENC	.000	2	0	19951201	19951201	UADT < ou = ISDT
Mise à jour 1 de l'édition 2	.001	2	1	Annulée	19960429	ISDT seulement

Les fournisseurs de données doivent extraire les informations nécessaires du champ DSID avant le chiffrement et les coder dans le CATD-COMT du fichier CATALOG.031. La structure et le format de ce champ est décrit en plus amples détails dans la section 6.4.1. Les systèmes des clients utilisateurs de données doivent donc lire le champ CATD-COMT comme s'ils avaient accès au champ DSID d'un ensemble de données d'échange déchiffré.

6.4.1 La structure et le format du CATD-COMT

Les informations DSID stockées dans le champ CATD-COMT sont sous-divisées en 4 ou 5 sous-champs séparés par une virgule.

Exemples :

```
VERSION=1.0,EDTN=1,UPDN=0,UADT=20060703,ISDT=20060703 ;
VERSION=1.0,EDTN=1,UPDN=1,ISDT=20060710 ;
```

6.4.1.1 Codage des cellules annulées (voir également les sections 6.2.3. et 6.2.3.1)

Etant donné qu'une mise à jour ne contenant que le message supprimé est fourni, il devrait être traité comme un ER. En conséquence, en ce qui concerne le champ CATD-COMT, il devrait être codé comme suit :

```
VERSION=1.0,EDTN=0,UPDN=2,ISDT=20060814;
```

Le tableau suivant illustre les conditions qui s'appliquent à tous les différents types de transactions.

Numéro de version	Numéro d'édition	Numéro de mise à jour	Date d'application de la mise à jour [UADT]	Date d'édition [ISDT]	Commentaire
VERSION=1.0	EDTN=1	UPDN=0	UADT=20060703	ISDT=20060703	Nouvelle cellule (EN)
VERSION=1.0	EDTN=1	UPDN=1	Annulée	ISDT=20060710	Mise à jour (ER)
VERSION=1.0	EDTN=1	UPDN=10	UADT=20060710	ISDT=20060717	Réédition (EN)
VERSION=1.0	EDTN=1	UPDN=11	Annulée	ISDT=20060724	Mise à jour (ER)
VERSION=1.0	EDTN=2	UPDN=0	UADT=20060731	ISDT=20060731	Nouvelle édition (EN)
VERSION=1.0	EDTN=2	UPDN=1	Annulée	ISDT=20060807	Mise à jour (ER)
VERSION=1.0	EDTN=0	UPDN=2	Annulée	ISDT=20060814	Cellule supprimée (ER)

6.5 Gestion de la mise à jour des ENC

Un dossier est fourni qui permet aux clients utilisateurs de données de vérifier la compatibilité et la capacité d'un ensemble de données d'échange d'une mise à jour d'ENC spécifique avant l'importation. Le client utilisateur de données peut utiliser ce dossier pour vérifier que les derniers ensembles de données d'échange de base sont compatibles avec la mise à jour installée en cours d'installation sur l'ECDIS. Ce dossier décrit l'état actuel de tous les ensembles de données de base associés à un service de fournisseur de données. Il est appelé STATUS.LST. La section suivante décrit plus en détails le format et le contenu.

6.5.1 Dossier STATUS.LST

Ce fichier est stocké dans le dossier INFO de l'ensemble de mises à jour d'échange fournies sur le média contenant un seul ensemble de données d'échange[10]. Il est fourni de façon à ce que les clients utilisateurs de données puissent vérifier l'état actuel du SENC par rapport aux données de base disponibles. Ce fichier peut être utilisé pour vérifier qu'un ensemble de mises à jour d'échange est compatible avec les derniers CD-ROM de base installé sur le système du client utilisateur de données.

6.5.1.1 Etat du format en-tête

L'en-tête est un enregistrement d'une longueur fixe qui contient les informations suivantes :

Champ ID	Domaine	Octets	Portée
ID du fournisseur de données	caractère	2	Tout caractère double alphanumérique
Semaine de parution	caractère	10	Tout caractère ASCII
Type de CD-ROM	caractère	10	UPDATE
Date de parution	décimal	8	YYYYMMDD
Délimiteur de fin d'enregistrement	hexadécimal	2	CR/LF

Exemple de l'état de l'en-tête:
GBWK15-08 UPDATE 20080403

6.5.1.2 Etat du format d'enregistrement

C'est un enregistrement séparé par une virgule avec un délimiteur de fin de ligne CR/LF :

Champ ID	Domaine	Octets	Portée
No du CD-ROM de base	caractère	2-3	alphanumérique
ID du fournisseur de données	caractère	2	alphanumérique
Dernière date de publication du CD-ROM de base	caractère	7	Tout caractère ASCII
Information lisible par l'homme	caractère	1-100	Chaîne de texte au format ASCII entre guillemets (') [HEX 27]
Date de publication du CD-ROM de base	décimal	8	YYYYMMDD
Delimiteur de fin d'enregistremetn	hexadécimal	2	CR/LF

Exemple d'état d'enregistrement:
`B1,GB,WK52-07,'BASE CD 1 dated 27 December 2007', 20071227`

Les systèmes doivent gérer de façon appropriée l'importation de données de base de différents fournisseurs de données et stocker les information des données de base installées. Lors du chargement de nouvelles mises à jour, les clients utilisateurs de données devront vérifier que les derniers CD-ROM de base listés dans ce fichier sont concordants avec ceux installés sur le système. Dans le cas contraire, le système doit rapporter un message du type suivant :

"Ce CD-ROM de mise à jour n'est pas compatible avec les ENC installées actuellement. Veuillez installer le CD-ROM de base <Numéro>, date <date>' et puis continuer le processus de mise à jour".

---

[10] Le support à grande capacité contient déjà un mécanisme destiné à gérer l'état de la SENC avec le fichier MEDIA.TXT.

Completer l'exemple[11]:

```
GBWK15-08   UPDATE    20080403
B1,GB,WK52-07,'BASE CD 1 dated 27 December 2007',20071227
B2,GB,WK14-08,'BASE CD 2 dated 03 April 2008',20080427
B3,GB,WK07-08,'BASE CD 3 dated 08 February 2008',20080227
B4,GB,WK07-08,'BASE CD 4 dated 08 February 2008',20080227
```

6.6 Le fichier Readme (README.TXT) de la S-57

Les fournisseurs de données utilisent actuellement le fichier README.TXT pour coder les informations importantes qui se rapportent à leurs services. Ces informations peuvent inclure:

1. Les informations de service général fournies par le fournisseur de données.
2. Les informations spécifiques fournies par les RENC et les producteurs individuels d'ENC concernant leurs données ENC.
3. Tout renseignement sur des données ENC spécifiques, telles que le chevauchement des ENC ou les questions identifiées sur des cellules spécifiques.

Bien que l'inclusion du fichier README.TXT ne soit pas prescrite dans la spécification de produit de la S-57, il est devenu une source importante d'informations en ce qui concerne l'ensemble des services commerciaux relatifs aux ENC, particulièrement étant donné la quantité accrue d'ENC disponibles provenant d'un grand nombre de pays producteurs différents.

Ayant ceci présent à l'esprit, il est fortement recommandé que les systèmes des clients utilisateurs de données puissent afficher ce fichier sur demande. Etant donné que ce fichier est relativement peu connu des utilisateurs, il serait utile pour le système des clients utilisateurs qu'il soit affiché au moment de l'installation des données ENC pour attirer forcément leur attention.

[11] La plupart des fournisseurs de données re-éditent à présent tous leurs CD-ROM de base simultanément ; il est admis que cela devrait évoluer vers une méthode incrémentale de publication des bases.

Page laissée en blanc intentionnellement

7 REPERTOIRE ET STRUCTURE DE FICHIER

7.1 Introduction

Le dispositif n'impose pas l'utilisation d'un répertoire particulier ou d'une structure de fichier. Toutefois, du fait que le fichier de données ENC est chiffré, il est difficile de maintenir certaines associations de fichier vitales, c'est-à-dire fichier texte et image avec les fichiers de cellule ENC appropriés (fichier de base ou mise à jour). La structure de répertoire qui a été adoptée par les fournisseurs de données existants est donnée en example ci-dessous à la section 7.5.1.1. Cette structure permet aux fichiers texte et images d'être gérée en maintenant une relation directe entre eux et le fichier correspondant ENC.

7.2 Gestion du fichier S-57

La structure du répertoire n'est pas obligatoire et peut varier entre fournisseurs de données. L'emplacement de tous les fichiers S-57 dans un ensemble de données d'échange chiffré est défini dans le CATALOG.031. C'est-à-dire que le chemin d'accès à tous les fichiers dans l'ensemble d'échange est spécifié dans chaque enregistrement de fichier.

7.3 Structure de fichier

Tout comme l'ensemble de données d'échange [ENC_ROOT] le répertoire racine contient un dossier nommé 'INFO' qui contient le fichier PRODUCTS.TXT (voir section 6.2), STATUS.LST (voir section 6.55) et tous les fichiers supplémentaires, ou extra, à définir, selon les spécifications des fournisseurs de données particuliers. Le répertoire racine contient également le fichier SERIAL.ENC (voir section 6.33). Chaque fichier de cellule ENC dans l'ensemble de données d'échange ENC_ROOT possède un fichier de signature correspondant. (voir section 5.3).

Les fournisseurs de données fournissent à présent le certificat d'authentification (.CRT) avec un ensemble de données d'échange chiffré S-63 pour soutenir les implémentations de l'édition 1.0 de la S-63. Le fichier de ce certificat est contenu dans le répertoire racine. L'édition 1.1 ne prévoit pas la fourniture de ce fichier avec des ensembles de données d'échange S-63. Les fournisseurs de données continueront de fournir ce fichier pendant une période limitée après quoi il sera retiré de leurs services.

Les fabricants peuvent toutefois programmer leurs systèmes pour détecter automatiquement un ensemble de données d'échange ou un groupe d'ensembles de données d'échange ; ceci ne doit pas être programmé spécifiquement dans le système. Si le média contient un format inattendu, le système doit aller par défaut à un logiciel de navigation de façon à ce que les utilisateurs puissent préciser manuellement la place du répertoire ENC_ROOT d'un ensemble de données d'échange requis. Un ensemble de données d'échange S-63 doit toujours contenir un dossier nommé ENC_ROOT qui doit contenir un seul fichier CATALOG.031 et au moins un fichier d'ensemble de données**.**

7.4 Dénomination des dossiers et fichiers

Tous les dossiers et fichiers doivent être dénommés selon les conventions définies dans la Spécification de production de la S-57 de l'OHI. Tous les dossiers et fichiers au sein d'un ensemble de données d'échange chiffré S-63 doivent être en MAJUSCULES.

7.5 Support des ensembles de données d'échange

Les fournisseurs de données peuvent fournir des ensembles de données d'échange aux clients utilisateurs de données en utilisant différentes méthodes, par exemple :

CD-ROM
Support à large capacité
Services en ligne

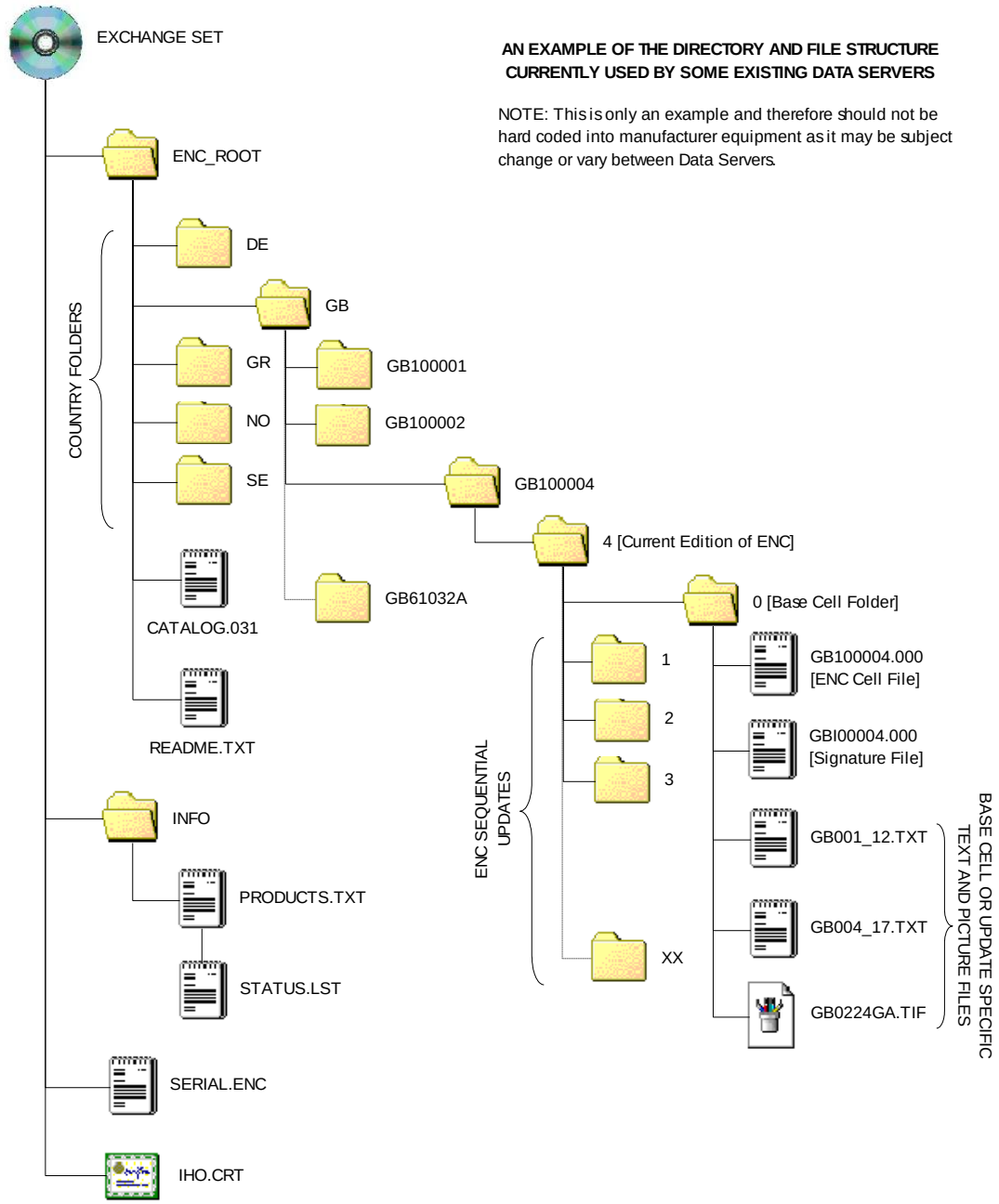
7.5.1 CD-ROM

On donnera aux ensembles d'échange chiffrés produits selon cette méthode un volume d'identification cohérent avec le dispositif de protection des données de la S-57 de l'OHI, c'est-à-dire. V01X03, V01X02, etc. La S-63 peut en tant qu'ensemble d'échange unique être livrée sur de multiples CD-ROM, mais l'expérience des fournisseurs de données a montré que ceci n'est pas recommandé. La méthode utilisée à présent par

certains fournisseurs de données est de publier des ensembles uniques de données sur de multiples CD-ROM.

7.5.1.1 Définitions des dossiers

Bien que l'example ci-dessous soit basé sur un CD-ROM de base, le CD-ROM de mise à jour est très similaire, la seule différence étant que la mise à jour ne tient pas nécessairement toutes les



NOTE: The location of all files in the exchange set [ENC_ROOT] can be read from the CATALOG.031 file

données de cellule de base. Cependant la mise à jour doit contenir des données qui soient cohérentes et en séquence avec le CD-ROM de base auquelle elle s'applique.

7.5.2 Supports à grande capacité

Les supports à grande capacité sont définis comme des périphériques capables de stocker de beaucoup plus gros volumes de données qu'un CD-ROM standard. Les renseignements portant sur le stockage des ENC chiffrées selon la S-63 sur de tels périphériques sont donnés en Appendice 2.

7.5.3 Services en ligne

Les clients utilisateurs de données peuvent télécharger des ensembles de données d'échange à partir du RENC/VAR commme indiqué par le fournisseur de service. Le téléchargement est ensuite copié sur un support rigide et, selon le support, le RENC/VAR indiquera le volume de l'identification à assigner au support. Il faut redire que tout ensemble d'échange copié [ENC_ROOT] doit tout le temps se conformer à la section 5.4, de l'Appendice B, de la S-57 de l'OHI, Spécifications de produit.

Page laissée en blanc intentionnellement

8. TACHES (PROCESSUS) DE L'ADMINISTRATEUR DU DISPOSITIF

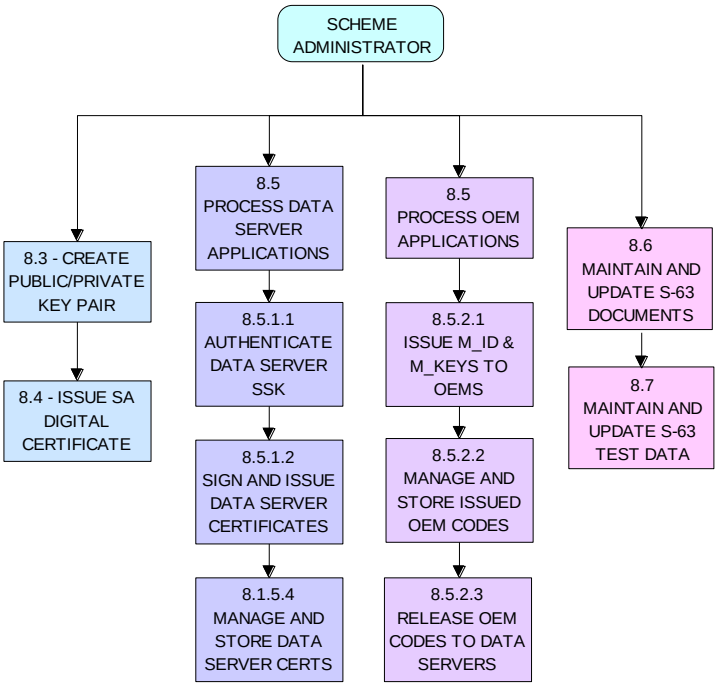
8.1 Administrateur du dispositif de protection des données

L'Administrateur du dispositif de protection des données (SA) est l'unique responsable de la tenue à jour et de la coordination de la S-63 - Dispositif de protection des données (DPS). Le rôle d'administrateur du dispositif est assuré par le Bureau hydrographique international (BHI), agissant en tant que secrétariat de l'OHI, au nom des Etats membres de l'OHI.

Le SA est chargé de contrôler les adhésions au dispositif et de faire en sorte que l'ensemble des participants appliquent les procédures définies. Le SA met à jour les clés de chiffrement dites « top level » qui sont utilisées pour exploiter le dispositif complet de protection des données et il est le seul organe qui est habilité à émettre des certificats destinés aux autres participants. Le SA est le garant de toute la documentation relative au dispositif.

8.2 Processus de l'Administrateur du dispositif de protection des données

Les principales responsabilités de l'OHI en tant qu'Administrateur du dispositif de la S-63 sont décrites dans le diagramme ci-dessous. Chaque « case du processus » établit une référence croisée avec la section particulière où ces opérations sont indiquées plus en détail.



Main Scheme Administrator Processes

8.3 Créer une paire de clé dite "top level » (de premier niveau)

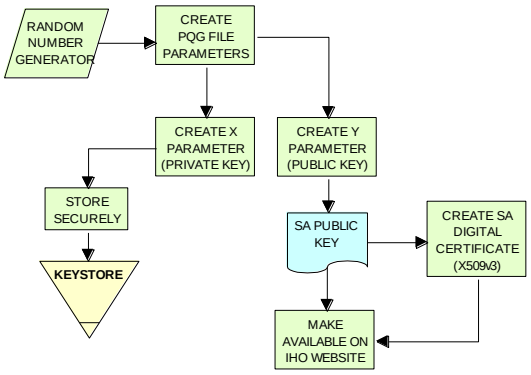
L'OHI en tant qu'Administrateur du dispositif doit créer une paire de clés privée et publique dite « top level » "de premier niveau". La clé privée sera utilisée pour signer les certificats de fournisseurs de données et la clé publique pour authentifier la signature. La clé publique doit être installée sur le système du client utilisateur de données indépendamment des données ENC chiffrées.

8.3.1 Créer les paramètres PQG

Cette procédure est normalement exécutée par le SA et les fournisseurs de données au cours de la création des paires de clés privée et publique. Bien qu'il ne soit pas nécessaire que les paramètres PQG générés par les fournisseurs de données soient identiques à ceux de la clé publique de SA et du certificat numérique de SA, les longueurs des clés utilisées doivent être identiques.

Le fichier PQG n'a d'existence à part entière que pendant la courte période de création des fichiers X et Y. Une fois ces derniers créés, le fichier PQG se trouvera dans les fichiers X et Y.

La création des paramètres appropriés PQG est décrite plus en détail dans la publication Norme de signature numérique (DSS) [2]. Pour de plus amples informations relatives au format du fichier PQG voir la section 5.4.2.1.



Make Top Level Key Pair

8.3.2 Créer la clé privée

La clé privée est un résultat du processus de génération de clés. La clé privée doit être stockée de façon sécurisée et accessible aux seules personnes qui ont besoin de la connaître. La possession non autorisée de la clé publique de SA peut potentiellement entamer la sécurité de la partie authentification du dispositif de protection des données. Le SA émettra une nouvelle clé publique (et le certificat de SA correspondant) si la clé privée est modifiée. Pour de plus amples informations sur le format de fichier X (clé privée) voir la section 5.4.2.2.

8.3.3 Créer la clé publique

La clé publique est un résultat du processus de génération de clés. La clé publique est envoyée à tous les participants au dispositif de protection des données, à la fois sous forme numérique et papier et chacune par différents moyens. Pour de plus amples informations sur le format de fichier Y (clé publique) voir la section 5.4.2.3.

8.4 Créer et publier un certificat numérique de SA (X509v3)

Le certificat numérique de SA sera conforme à X509v3 [4]. Le certificat numérique sera toujours fourni dans un fichier appelé IHO.CRT. Le fichier IHO.CRT est disponible sur le site web de l'OHI http://www.iho.int.

Le SA utilise une clé publique de DSA d'une longueur de 512 bits.

Tous les fournisseurs de données qui fournissent un service ENC peuvent inclure le certificat de SA, pour référence, dans le répertoire racine du support (c'est-à-dire en D:\IHO.CRT sur un CD-ROM) mais, comme indiqué dans la Section 6.1, l'installation du certificat de SA sur le système d'un client utilisateur de données devrait être effectuée indépendamment. Le contrôle de validité de la signature du SA au sein de chaque fichier de signature ENC doit être exécuté à partir de la version du certificat de SA installée indépendamment.

La clé publique de SA (contrairement au certificat numérique) est également mise à disposition en tant que fichier ASCII sur le site web de l'OHI http://www.iho.int (le format est décrit à la Section 6.5).

8.4.1 Mise à jour du certificat numérique de SA X509v3 (clé publique)

Le SA publiera et mettra à disposition un nouveau certificat numérique de SA dans les circonstances suivantes :

- Lorsque le certificat numérique du SA vient à expiration. Dans ce cas, le certificat ne devra pas contenir une clé publique modifiée.
- Lorsque la clé privée du SA a été modifiée. Dans ce cas, une nouvelle clé publique devra être contenue à l'intérieur du certificat numérique du SA. hen the SA private key has been compromised. In this case a new public key shall be contained within the SA Digital Certificate.

Le SA publiera son nouveau certificat numérique et, si applicable, une nouvelle version imprimée (réf. section 6.5) de la clé publique sur le site web de l'OHI (http://www.iho.int). Tous les fournisseurs de données et les fabricants seront immédiatement informés et recevront des exemplaires du nouveau certificat numérique et, si applicable, la nouvelle clé publique sous forme imprimable.

Le fournisseur de données et les fabricants sont collectivement responsables d'informer leurs clients utilisateurs de données de tout nouveau certificat numérique de SA et, si besoin est, de toute nouvelle clé publique de SA.

Cette procédure est normalement réalisée par tous les utilisateurs du dispositif de protection lorsqu'un nouveau certificat numérique de SA ou une clé publique est publiée et est réalisée comme suit :

- Obtenir le nouveau certificat numérique de SA et la clé publique de SA imprimable à partir du site web de l'OHI (http://www.iho.int).
- L'application doit charger le nouveau certificat numérique de SA et contrôler que la clé publique et la clé publique imprimable sont identiques. Une fois seulement que cela a été fait, l'application garantit que la clé publique de SA est correcte. Ce même processus est appliqué au remplacement de la clé publique originale du SA.
- Remplacer le certificat numérique existant par le nouveau certificat émis**.**

8.5 Traitement des demandes d'adhésion des fournisseurs de données et des fabricants

L'Administrateur du dispositif est responsable du traitement des demandes d'adhésion des fournisseurs de données et des fabricants qui souhaitent s'abonner au dispositif de protection des données ENC de l'OHI. Ceci inclut la gestion et l'émission de certificats signés par le SA aux fournisseurs de données et la gestion et l'émission de codes de fabricant (M_ID & M_KEY) aux fabricants acceptés ainsi que leur diffusion aux fournisseurs de données autorisées. Les processus d'adhésion sont décrits plus en détail dans les **ANNEXE A** & **ANNEXE** B à ce document**.**

8.5.1 Traitement de la demande de certificat de fournisseur de données par le fournisseur de données

Il sera nécessaire que le candidat ait réussi à devenir fournisseur de données pour fournir un certificat signé avec la clé privée de fournisseur de données, connue sous le nom de clé auto-signée (SSK). Le processus de certification est exécuté par le SA et décrit étape par étape ci-dessous :

8.5.1.1 Authentifier le fichier de clé auto-signée (SSK)

Le SA authentifie le fichier SSK du fournisseur de données avant de créeer et d'émettre un certificat de fournisseur de données. D'abord, le SA doit confirmer que la SSK a été fournie dans le format correct décrit dans la section 5.4.2.5, si le format est incorrect, il faudra mettre fin au processus et un avertissement devra être donné. Si le format est exact, le processus d'authentification se déroulera comme suit :

a) Extraire les élements de signature 'R' et 'S' (c'et-à-dire les deux premières chaînes de données et leurs en-têtes attenant du fichier SSK fourni par le fournisseur de données). Ceci donne un fichier de clé publique.
b) Hacher le fichier de clé publique en utilisant l'algorithme SHA-1. Tous les octets à l'intérieur du fichier doivent être hachés.
c) Vérifier la signature (les éléments supprimés en « a » ci-dessus) en la passant avec le fichier de clé publique et le résultat du hachage du fichier de clé publique (tel qu'obtenu en 'b' ci-dessus) au travers du *DSA* [2]. Ceci fournit en retour l'état (correct ou incorrect).

Si la signature est correcte, le SA peut produire le certificat de fournisseur de données.

8.5.1.2 Créer le certificat de fournisseur de données

Le SA crée un certificat de fournisseur de données après que le SSK ait été authentifié. Les détails de l'algorithme DSA de signature sont décrits dans la publication FIPS 186 Norme de signature numérique (DSS). La procédure est la suivante :

a) Eliminer les éléments de signature (c'est-à-dire les deux premières chaînes de données et leurs en-têtes attenants) du fichier de clé auto-signée. Ceci donne le fichier de clé publique.
b) Hacher le fichier de clé publique en utilisant l'algorithme *SHA-1* [3]. Tous les octets à l'intérieur du fichier doivent être hachés.

c) Signer le fichier de clé publique (tel que hâché en 'b' au-dessus) en passant la clé privée de SA, le fichier haché de la clé publique (tel qu'obtenu en 'b' ci-dessus) et une chaîne aléatoire au travers du *DSA* [2]. Ceci fournit en retour les deux éléments de signature ('R' et 'S').

d) Insérer ces éléments dans le fichier de certificat et y ajouter le fichier de clé publique (tel qu'obtenu en 'a' ci-dessus) pour former le certificat.

8.5.1.3 Authentifier le certificat de fournisseur de données signé par le SA

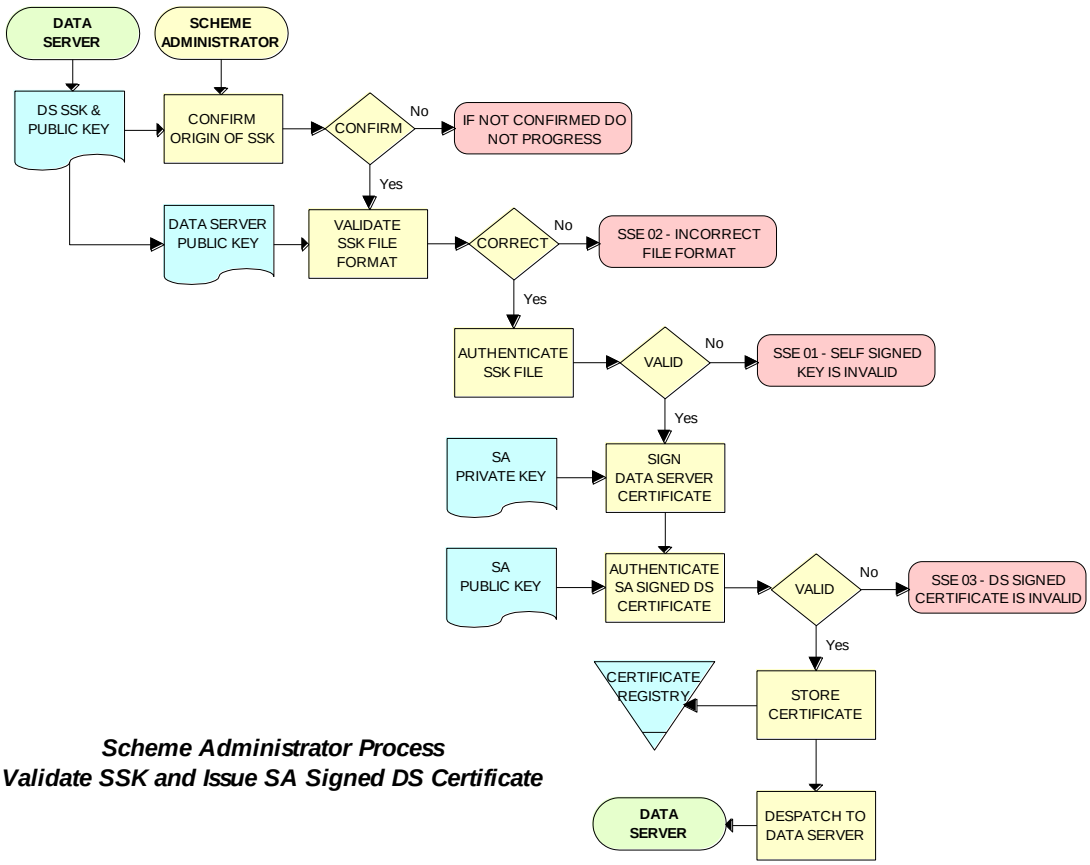
Le SA confirme que le certificat nouvellement signé est valide avant de le faire parvenir au fournisseur de données. La procédure est la suivante :

a) Extraire les éléments de signature (c'est-à-dire les deux premières chaînes de données et leurs en-têtes attenants) du fichier de certificat de fournisseur de données nouvellement créé. Ceci donne un fichier de clé publique.

b) Hacher le fichier de clé publique (obtenu de 'a') en utilisant l'algorithme *SHA-1*. Tous les octets à l'intérieur du fichier doivent être hachés.

c) Vérifier les éléments de signature (tels que obtenus en 'a' ci-dessus) en les passant, ainsi que la clé publique de SA (telle qu'obtenue en 'a') et le résultat du hachage du fichier de clé publique (tel qu'obtenu en 'b' ci-dessus) au travers du *DSA* Ceci fournit en retour un état (correct ou incorrect).

Si le certificat de fournisseur de données est authentifié correctement, il peut être envoyé au fournisseur de données et utilisé dans la construction de de signatures numériques ENC.



Scheme Administrator Process
Validate SSK and Issue SA Signed DS Certificate

8.5.1.4 Gérer les certificats de fournisseur de données

Lorsqu'un certificat de fournisseur de données nouvellement signé par le SA a été publié, il doit être stocké dans des archives de certificats. Le certificat devra être uniquement assigné au fournisseur de données et comportera des références croisées avec la clé privée utilisée pour le signer et avec la clé publique utilisée pour confirmer son authentification.

8.5.2 Traitement de la demande d'adhésion du fabricant

Les fabricants doivent déposer une demande d'adhésion au SA pour devenir membre du dispositif de protection des données de l'OHI (S-63).

8.5.2.1 Publication et gestion des codes fabricants de la S-63

On remettra aux candidats ayant réussi à devenir fabricants leur propre identification unique de fabricant (M_ID) et leur clé de fabricant (M_KEY) voir sections 4.2.4 et 4.2.5. Ces codes doivent être stockés de façon sécurisée ainsi que les renseignements relatifs aux fabricants et à leur participation active au dispositif.

8.5.2.2 Publication des listings M_ID et M_KEY aux fournisseurs de données

Les fournisseurs de données ont besoin des valeurs M_ID et M_KEY de façon à pouvoir identifier un fabricant particulier et obtenir la M_KEY correcte pour extraire le HW_ID du client utilisateur de données à partir du permis d'utilisateur. Le SA donnera aux fournisseurs de données une liste complète de codes pour tous les fabricants approuvés des systèmes conformes à la S-63. Cette liste sera fournie sous une forme protégée chaque fois qu'un fabricant sera ajoutée à la liste ou si le statut d'un fabricant change, par exemple si son adhésion au dispositif est annulée.

8.6 Données d'essai de la S-63

Le dispositif de protection des données de la S-63 est appuyé par un ensemble exhaustif de données d'essai, voir S-63 Appendice 1 – Données d'essai du dispositif de protection des données.

8.7 Administrateur du dispositif – Procédure de sécurité relative à l'assurance qualité

8.7.1 Documentation

Le SA doit conserver la documentation relative au dispositif de protection des données. Ceci doit être fait selon une procédure de contrôle des changements et le SA doit informer tous les participants au dispositif de protection des données (fournisseurs de données et développeurs d'applications pour les clients utilisateurs de données) des changements à la norme.

Les données d'essai concernant le dispositif de protection des données ainsi que le logiciel central sont également à la disposition des fabricants de système afin qu'ils puissent tester l'entière compatibilité de leur version. Les données d'essai et le logiciel central sont décrits dans les appendices A et B et sont disponibles sur le site web de l'OHI : (http://www.iho.int).

8.7.2 Gestion du contrat de confidentialité

Tous les détails requis pour exploiter le dispositif de sécurité ainsi que toutes les informations particulières (c'est-à-dire M_KEY) seront fournis aux parties concernées sous couvert du contrat de confidentialité. Le SA sera responsable de la gestion de ce contrat. Le contrat de confidentialité limitera pour les participants la possibilité de rompre le dispositif de protection des données**.**

8.7.3 Audit des registres de sécurité

Le SA aura la capacité de vérifier tous les registres de sécurité tenus par les participants au dispositif de protection des données. Le contenu de ces registres et défini dans les sections 0, 9.3.3.3, 0 et 10.10.3. Le SA verifiera ces registres pour confirmer qu'ils sont complets et à jour. Tout problème doit être corrigé immédiatement, faute de quoi le participant deviendra non conforme et pourra éventuellement être retiré du dispositif.de protection.

8.7.4 Création des M_IDs et M_KEYs

Le SA sera responsable de la création et de l'émission des valeurs M_ID et M_KEY utilisées au sein du dispositif de protection des données. Le SA enregistrera, dans un registre M_ID/M_KEY toutes les valeurs M_ID/M_KEY ainsi que les orgaisations qui les ont reçues. Le SA fera en sorte qu'aucune valeur ne soit créée en double.

Le SA fournira à tous les fournisseurs de données du dispositif de sécurité les informations sur les amendements aux valeurs M_ID et M_KEY**.**

8.7.5 Création des clés de signature numérique (clés privées et clés publiques)

Le SA aura la capacité de créer sa propre paire de clés publique et privée. La clé privée est utilisée au cours du processus de signature du certificat et la clé publique au cours du processus d'authentification de la signature.

La clé privée doit être stockée de façon sécurisée et accessible seulement aux personnes qui ont « besoin de la connaître». Le SA émettra une nouvelle clé publique (et un certificat de SA correspondant).

La clé publique de SA doit être mise à disposition de tous les participants au dispositif de protection des données (S-63) à la fois sous forme numérique et papier, c'est-à-dire fax et téléchargement à partir d'un site web. Les deux formats doivent être envoyés ou mis à disposition par différents moyens.

8.7.6 Acceptation des clés auto-signées (SSK)

Le SA devra confirmer que toute clé auto-signée fournie par le fournisseur de données est véritable en contactant l'organisation qui en est à l'origine. Ceci peut être fait par téléphone, télécopie ou courrier mais l'origine doit être confirmée au SA avant que le certificat de fournisseur de données ne soit signé par le SA à l'aide de la clé auto-signée. Le SA doit enregistrer les SSK reçues dans un Registre SSK.

8.7.7 Création de certificats de fournisseur de données

Le SA doit pouvoir créer les certificats de fournisseur de données signé par le SA à partir des clés auto-signées fournies par le fournisseur de données et la clé privée du SA. Le certificat signé devra être authentifié par rapport à la clé publique du fournisseur de données avant d'être envoyé au fournisseur de données. Le SA doit garder un enregistrement de tous les certificats de SA dans un Registre de certificat de fournisseur de données.

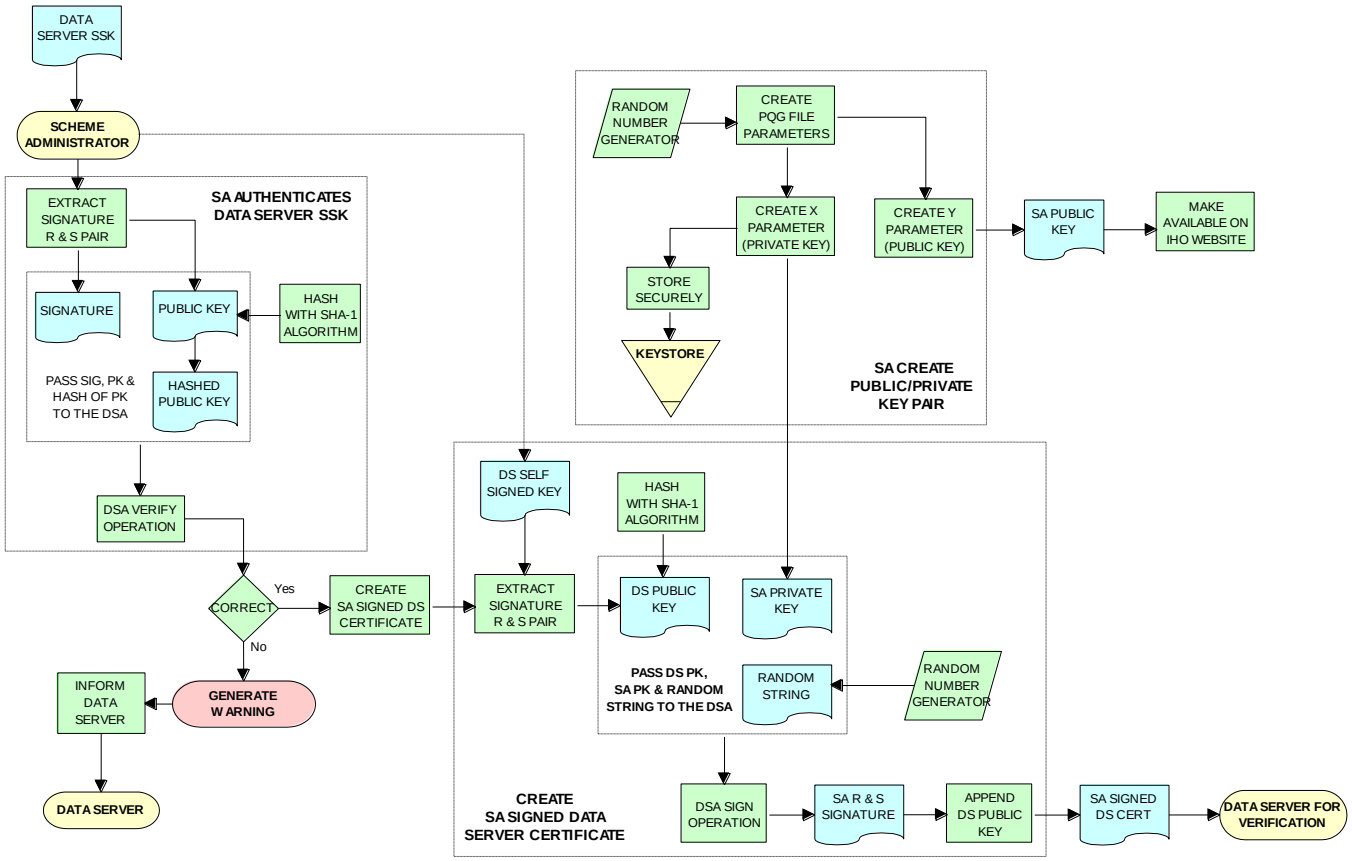
Le fournisseur de données devra signer un contre de confidentialité avant que le SA n'émette le certificat de fournisseur de données. Le SA fournira à tous les participants au dispositif de protection des informations sur tous les certificats de fournisseur de données annulés**.**

8.7.8 Création de chaînes aléatoires

Pour signer les données (requis dans le cadre de la création de certificat), le SA devra créer des chaînes aléatoires. Le SA fera en sorte que la même valeur ne soit pas utilisée pour deux signatures distinctes, bien que ceci ne puisse être garanti si les chaînes sont créées de manière aléatoire. Cependant, la probabilité que la même chaîne soit créée deux fois est extrêmement ténue.

8.7.9 Remise de M_ID et M_KEY

Lorsqu'un fabricant de systèmes a achevé les tests de conformité interne, il lui sera demandé de signer un contrat de confidentialité avant que le SA n'émette les M_ID et M_KEY.



Scheme Administrator (SA) - SSK Authentication & Certificate Signing Process

Page laissée en blanc intentionnellement

9. PROCESSUS (TACHES) DU FOURNISSEUR DE DONNEES

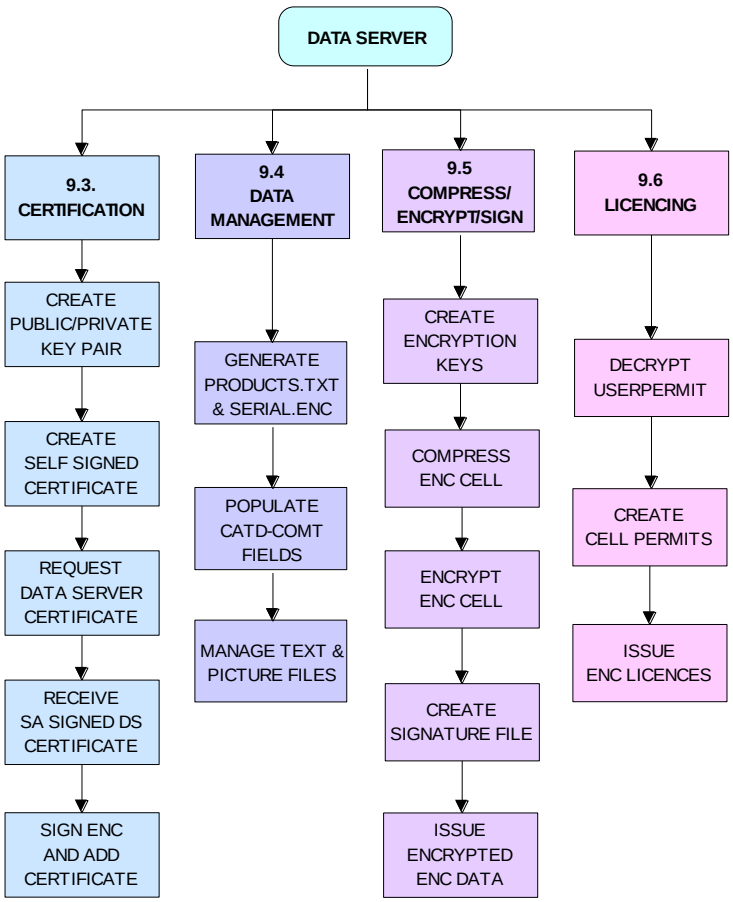
9.1 Vue d'ensemble

Les fournisseurs de données sont responsables du chiffrement et de la signature des informations ENC conformément aux procédures et aux méthodes définies dans la norme de l'OHI S-63 – Dispositif de protection des données.

Les Services hydrographiques et les organisations RENC sont des exemples de fournisseurs de données. Les organisations qui souhaitent devenir fournisseurs de données doivent d'abord signer et présenter un *contrat de fournisseur de données de la S-63* ainsi qu'un formulaire rempli de *demande de certificat de fournisseur de données*. Ce processus est décrit avec de plus amples détails sur le site web de l'OHI (www.iho.int).

9.2 Processus (taches) du fournisseur de données

Les pricipales responsabilités des fournisseurs de données agréés dans le cadre de la norme S-63 de l'OHI – Dispositif de protection des données sont décrites dans le diagramme suivant. Chaque « *cadre du processus* » dit « top level » établit des références croisées avec la section spécifique où ces opérations sont décrites avec plus détails**.**



Main Data Server Processes

9.3 Processus de certification

9.3.1 Produire une paire de clés publiques/privées

Les fournisseurs de données devront créer une paire de clés privées et publiques en tant que partie intégrante de la méthodologie de chiffrement « asymétrique » adoptée par la norme S-63 de l'OHI - Dispositif de protection des données. Les clés publiques et privées du fournisseur de données sont utilisées dans les fonctions suivantes :

- La clé privée est utilisée pour signer la clé publique du fournisseur de données en vue de créer un certificat auto-signé (SSK).
- La clé publique est utilisée pour valider le SSK avant qu'il ne soit fourni au SA.
- La clé privée est utilisée pour signer tous les fichiers de données compressés et chiffrés produits par le fournisseur de données.
- La clé publique est utilisée pour contrôler l'intégrité des fichiers de données ENC dans l'ECS/ECDIS.

9.3.1.1 Créer des paramètres de signature PQG

Cette procédure est normalement suivie par le SA et les fournisseurs de données lors de la création des paires de clés publiques/privées. Bien qu'il ne soit pas nécessaire que les paramètres générés par les fournisseurs de données soient identiques à ceux contenus dans la clé publique de SA et le certificat numérique de SA, la longueur des clés utilisées doit être identique.

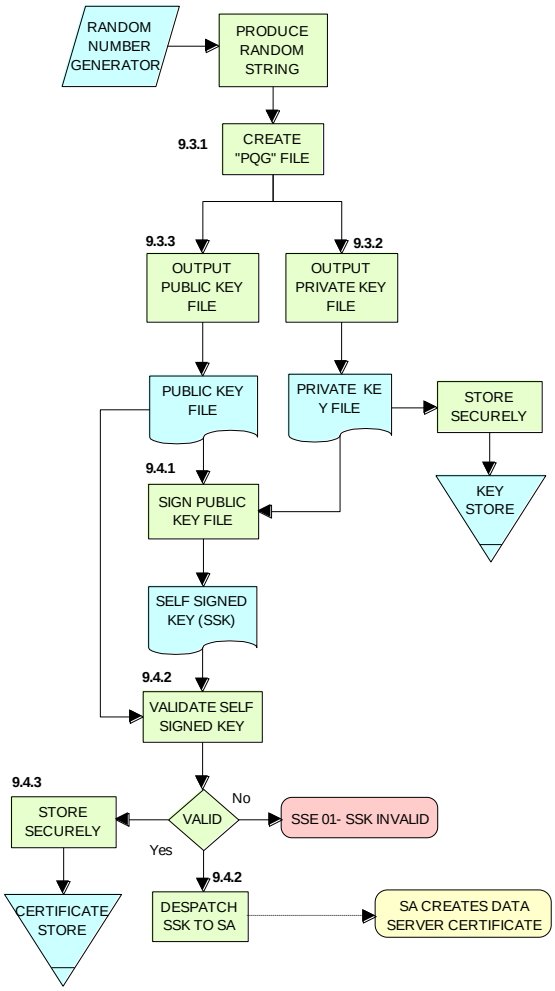
Le fichier PQG existe en tant que tel que pendant une courte période lors de la création des fichiers X et Y. Après que ceux-ci aient été créés, le fichier PQG sera contenu dans les fichiers X et Y.

La création des paramètres PQG est décrite dans la publication Norme de signature numérique (DSS [2].

9.3.1.2 Créer un fichier de clé privée

La clé privée est le résultat du processus de génération des paramètres PQG. La clé privée doit être stockée de façon sécurisée et son accès limité aux seules personnes qui ont besoin de la connaître.

La possession non autorisée de la clé privée du fournisseur de données peut potentiellement fragiliser la sécurité de la partie relative à l'authentification du dispositif. Le fournisseur de données émettra une nouvelle clé publique si la clé privée est modifiée. Le fournisseur de données. Des renseignements relatifs au format de fichier X (clé privée) se trouvent en section 5.4.2.2.



Data Server Processes
Create Public/Private Key Pair
Produce & Authenticate Self Signed Key (SSK)

9.3.1.3 Créer un fichier de clé publique

La clé publique est le résultat du processus de génération des paramètres PQG. La clé publique est contenue dans le certificat de fournisseur de données signé par le SA qui fait partie du fichier de signature ENC (voir section 5.4.2.7**Erreur ! Source du renvoi introuvable.**). Le système des clients fournisseurs de données extrait l'élément de clé publique de ce fichier pour contrôler l'intégrité du fichier de donnée ENC par rapport à la signature ENC. Des renseignements relatifs au format de fichier Y (clé publique) se trouvent en section 5.4.2.3.

9.3.2 Créer une clé auto-signée de fournisseur de données (SSK)

La SSK est créée et présentée au SA pour obtenir un certificat de fournisseur de donnée. La SSK contient la clé publique de fournisseur de données avec une signature créée par le fournisseur de données.Bien que le format SSK soit identique au certificat de fournisseur de données défini à la section 0, la seule différence est que la SSK est créée par le fournisseur de données et que le certificat de fournisseur de données est créé et émis par le SA.

La SSK définit la signature de la clé publique du fournisseur de données. Le passage à la signature doit être la clé publique du fournisseur de données, formatée selon le format de fichier de clé publique tel que décrit à la section 5.4.2.3. Le fichier SSK file sera écrit en langage ASCII avec le format, la structure et l'ordre décrit à la section 5.4.2.5.

9.3.2.1 Signer la clé publique et générer la SSK

Cette procédure est normalement effectuée une fois par le fournisseur de données pour créer sa clé auto-signée (SSK) ; qui est ensuite envoyée au SA qui l'utilisera pour créer le certificat de fournisseur de données. Les détails de l'algorithme DSA de la signature numérique sont fournis dans la publication FIPS 186 Norme de signature numérique (DSS) [2]. La procédure est la suivante :

a) Hacher le fichier de clé publique en utilisation l'algorithme *SHA-1* [3]. Tous les octets à l'intérieur du fichier doivent être hachés.
b) Signer le fichier de clé publique (tel que haché en « a » en envoyant le fichier de clé privée, le hachage du fichier de clé publique (tel qu'obtenu en « a » ci-dessus et une chaîne aléatoire à travers l'algorithme DSA [2]. Ceci restituera les deux éléments de signature ('R' et 'S').
c) Ecrire ces éléments dans le fichier de clé auto-signée dans le format défini en section 5.4.2.5 et ajouter le fichier de clé publique pour former le fichier de clé auto-signée.

9.3.2.2 Authentifier/Valider la SSK du fournisseur de données

Les fournisseurs de données doivent authentifier la SSK par rapport à la clé publique de fournisseur de données pour confirmer qu'une SSK valide a été produite.

a) Extraire les élémets de signature 'R' et 'S' (c'est-à-dire les deux premières chaînes de données et leurs en-têtes attenants du fichier SSK fourni par le fournisseur de données). Ceci donne le fichier de clé publique.
b) Hacher le fichier de clé publique en utilisat l'algorithme SHA-1 [3]. Tous les octets à l'intérieur du fichier doivent être hachés.
c) Vérifier la signature (les éléments supprimés en « a » ci-dessus) en la passant, avec le fichier de clé publique et le hachage (tel qu'obtenu en « b » ci-dessus), au travers du DSA. Ceci fournira en retour l'état correct ou incorrect.

Si la SSK est valide alors le SA peut fournir un exemplaire de la clé publique de fournisseur de données.

9.3.2.3 Stocker la clé auto-signée

Toute SSK produite par le fournisseur de données doit être stockée de façon sécurisée dans un *Registre de certificats* et une référence croisée doit être établie avec la paire associée de clés publique et privée.

9.3.3 Valider les certificats

9.3.3.1 Authentifier le certificat numérique X509 du SA

Cette procédure est réalisée par:

a) Les fournisseurs de données, en tant que partie de la vérification de la clé publique du SA nécessaire pour authentifier le certificat de fournisseur de données.
b) Les clients utilisateurs de données pour vérifier la clé publique de SA à utiliser pour authentifier les signatures numériques fournies avec les données ENC.

La procédure du fournisseur de données est la suivante :

Comparer manuellement la clé publique de SA contenue à l'intérieur du certificat numérique du SA avec une copie de la clé publique imprimable disponible à partir du site web de l'OHI (http://www.iho.int). Si le contrôle ci-dessus échoue, le fournisseur de données n'acceptera pas le certificat numérique du SA. Sinon, le certificat numérique du SA est valide et la clé publique du fournisseur de données qu'il contient peut être utilisée pour produire les fichiers de signature ENC.

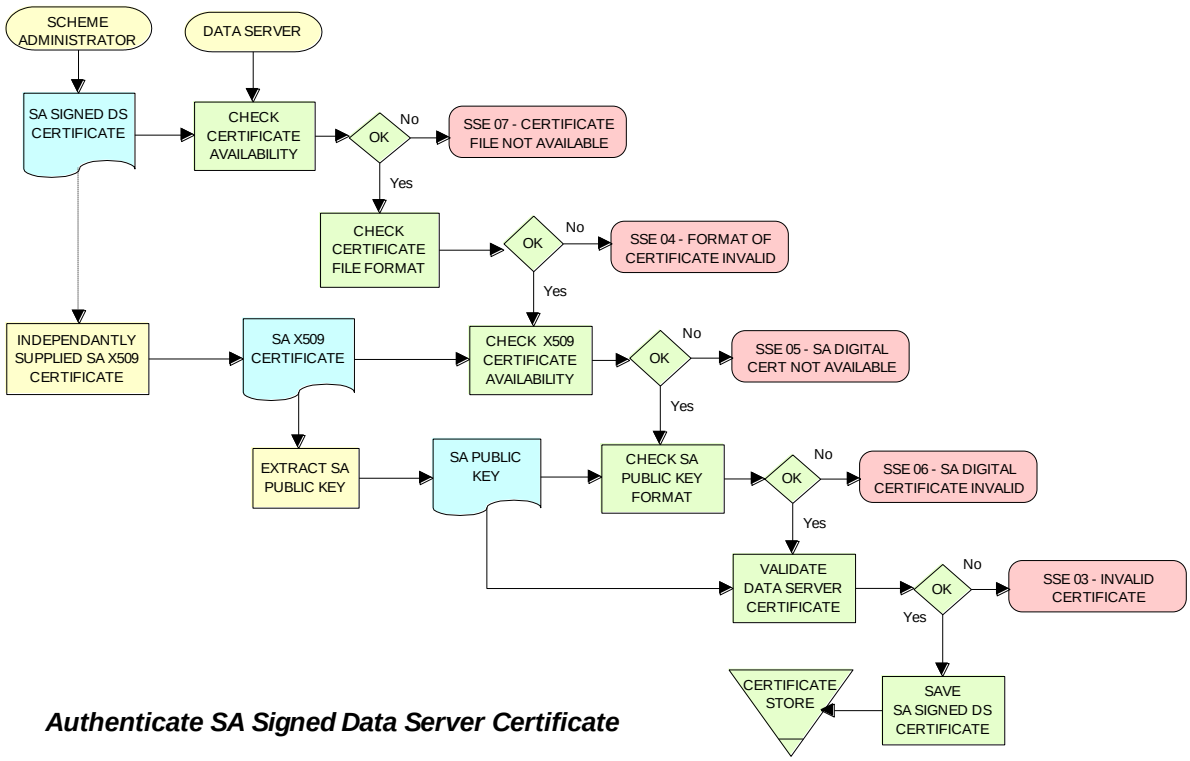
9.3.3.2 Authentifier le certificat de fournisseur de données signé par le SA

Cette procédure est réalisée par les fournisseurs de données pour authentifier le certificat obtenu du SA avant de l'utiliser. Si les fournisseurs de données utilisent des moyens automatisés d'authentification alors le logiciel employé devra contrôler en premier lieu :

a) Qu'il y a un certificat à authentifier
b) S'il y en a un, qu'il est au format correct tel que décrit dans la section 5.4.2.6

Si l'une ou l'autre de ces deux options sont négative, il doit être mis fin au processus et un avertissement approprié est donné. Sinon le processus d'authentification doit se dérouiler comme suit :

a) Obtenir la clé publique de SA à partir du site web de l'OHI : http://www.iho.int.
b) Extraire les éléments de signature (c'est-à-dire les deux premières chaînes de données et leurs en-têtes attenants) du fichier de certificat. Ceci donne un fichier de clé publique.
c) Hacher le fichier de clé publique (obtenu de 'b') en utilisant l'algorithm SHA-1 [3]. Tous les octets à l'intérieur du fichier doivent être hachés.
d) Vérifier les éléments de signature (tels qu'obtenus en 'a' ci-dessus) en les passant, ainsi que la clé publique de SA (tel qu'obtenue en « b » ci-dessus) au travers du DSA [2]. Ceci fournit en retour un état (correct ou incorrect).
e) Si le certificat de fournisseur de données est authentifié correctement, ses éléments de signature 'R' et 'S' peuvent alors être utilisés dans la construction de signatures numériques ENC signatures**.**



Authenticate SA Signed Data Server Certificate

9.3.3.3 Stockage du certificat de fournisseur de données signé par le SA

Tous les certificats fournis par l'Administrateur du dispositif doivent être stockés de façon sécurisée dans un ***Registre de certificats*** et des références croisées doivent être établies avec la paire associée de clés publique/privée et la SSK.

9.4 Processus de gestion des données

Le processus de gestion des données comprend la création et la gestion de fichiers destinés à être inclus dans un ensemble de données d'échange chiffrées S-63, quil inclut les fichiers suivants :

a) Le fichier PRODUCTS.TXT (voir section 6.2)
b) Le fichier SERIAL.ENC (voir section 6.3)
c) Le champ CATD-COMT du fichier CATALOG.031 (voir section 6.4.1)
d) Fichier texte et image enregistré dans le fichier CATALOG.031 file (voir section 7.1)

Chacun d'eux demande une gestion rigoureuse à l'intérieur du logiciel de production du fournisseur de données et doit être généré conformément aux formats et aux conventions décrits en section 6.

9.5 Processus de chiffrement, de compression et de signature ENC

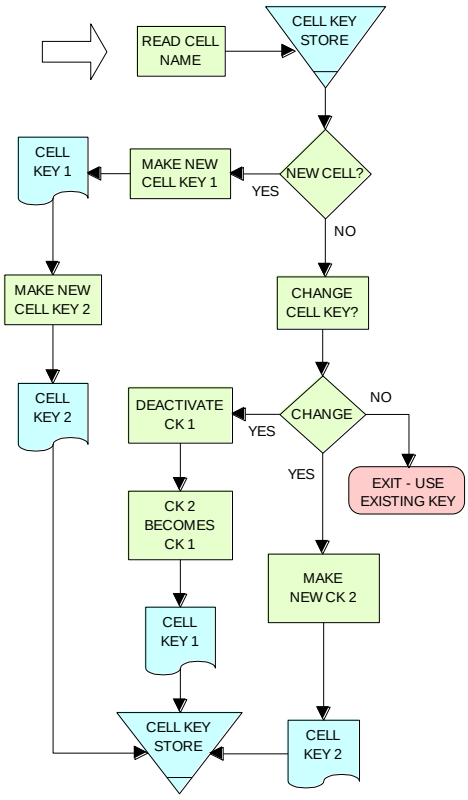
9.5.1 Gestion du chiffrement des clés de cellule (ECK)

Chaque ENC est chiffrée à l'aide d'une unique clé de cellule et chaque permis ENC peut stocker deux clés de cellule chiffrées. Ces clés peuvent être incrementées de temps en temps à la discrétion du fournisseur de service, et il est donc important de les gérer d'une façon efficiente et efficace.

Pour créer de nouvelles clés et incrémenter celles qui existent le fournisseur de données aura besoin d'une application pour gérer automatiquement els clés et les storer de façon sécurisée. Cette application doit pouvoir générer des chaînes aléatoires de la longueur correcte et dans l'idéal doit avoir un moyen de contrôler que des doubles de clés de cellule ne soient pas produits à l'intérieur d'un ensemble.

L'application doit pouvoir de créer de nouvelles clés de cellules et également gérer l'incrémentation des clés de cellule déjà en service. Les étapes suivantes montrent les processus logiques associés à la gestion des clés, et le diagramme ci-contre apporte un éclairage supplémentaire.

1. Obtenir le nom de cellule et, si nécessaire, le numéro d'édition et déterminer s'il s'agit d'une nouvelle cellule.
2. S'il s'agit d'une nouvelle cellule, faire de nouvelles clés 1 & 2, si non aller en 4.
3. Stocker les nouvelles clés dans le stock de clés.
4. S'il ne s'agit pas d'une nouvelle cellule, faut-il changer la clé ? Si non aller en 5, si oui aller en 6.
5. Sortir et continuer à utiliser les clés de cellule existantes.
6. La clé de cellule 1 est maintenant désactivée et la clé de cellule 2 devient clé de cellule 1 et elle est signalée comme telle dans le magasin de clés.
7. Créer une nouvelle clé de cellule 2 et l'ajouter au stock de clés.



Data Server Process
Create and Manage Cell Keys

NOTE: L'incrémentation des clés est à la discrétion du fournisseur de données et est basée sur les règles de gestion associée à la livraison du service.

Les clés pourront être incrémentées lorsque :

- les clés chiffrées ont été annulées.
- tous les ans ou à intervalle défini par le fournisseur de données.
- en synchronisation avec l'émission d'une nouvelle édition de cellule**.**

9.5.1.1 Format de clé de cellule

Les clés de cellule déchiffrées sont d'une longueur de 5 octets ou de 10 caractères hexadécimaux comme dans l'exemple ci-dessous.

Clé de cellule 1	C1CB518E9C	5 octets
Clé de cellule 2	421571CC66	5 octets

9.5.2 Compresser le fichier ENC (fichier de base base ou mise à jour)

Cette procédure est normalement réalisée par le fournisseur de données sur les fichiers ENC avant qu'ils ne soient chiffrés. La procédure est la suivante :

- Compresser le fichier de cellule ENC en utilisant la norme ZIP [6] décrite à (www.pkware.com).

Le fichier ENC compressé qui en résulte est utilisé comme une entrée dans l'étape de chiffrement du dispositif de protection. Seuls les fichiers de cellule ENC (fichier de base et mise à jour) sont compressés. Ce processus est toujours terminé avant que les données ne soient chiffrées et signées).

9.5.3 Chiffrer les fichiers ENC

9.5.3.1 Fichier de cellule de base

Cette procédure est réalisée par le fournisseur de données. Le fichier ENC doit être compressé avant d'être chiffré. La procédure est la suivante :

a) Sélectionner la ***clé de cellule*** à utiliser pour le chiffrement (voir les conditions en 9.5.1).
b) Chiffrer le fichier ENC en utilisant l'algorithme ***Blowfish*** avec la ***clé de cellule*** (résultant de 'a') pour créer un fichier ENC chiffré.

9.5.3.2 Fichier de mise à jour ENC

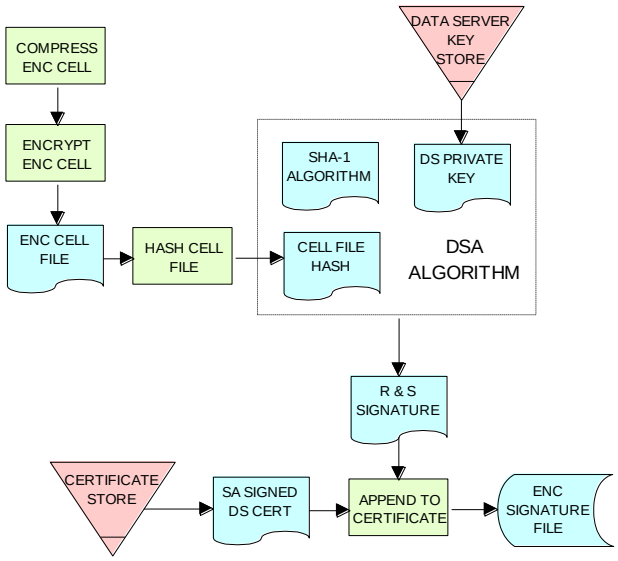
Cette procédure est réalisée par le fournisseur de données. Le fichier de mise à jour doit être compressé avant d'être chiffré. La procédure est la suivante :

a) Sélectionner la ***clé*** utilisée pour chiffrer le fichier de base auquelle la mise à jour s'applique.
b) Chiffrer le fichier de mise à jour ENC en utilisant l'algorithme ***Blowfish*** avec la ***clé*** (résultant de 'a') pour créer un fichier de mise à jour ENC chiffré.

9.5.4 Signer le fichier ENC (cellule de base ou mise à jour)

Cette procédure est réalisée par les fournisseurs de données pour signer numériquement leurs fichiers de données ENC. Les fichiers ENC doivent être compressés (sections 2 & 9.5.2) et chiffrés (sections 3 & 9.5.3) avant d'être signés. La procédure est la suivante :

a) Passer les contenus de la clé privée du fournisseur de données et du fichier ENC chiffré au travers de l'algorithme DSA [2]. L'algorithme DSA le fichier ENC chiffré en utilisant l'algorithme SHA-1 [3].
b) L'algorithme DSA fournit en retour deux paramètres de signature (R & S).
c) Enregistrer ces dernières comme les deux premières chaînes de données dans un fichier de signature conforme au format et aux conventions d'appellation définies à la section 5.4. Le reste du fichier doit être composé du certificat de fourisseur de données qui contient la clé publique associée à la clé privée utilisée pour créer la signature.



Process to Create ENC Signature Files

9.5.5 Emettre les données ENC chiffrées de la S-63

Les fournisseurs de données émettront les ensembles de données d'échange de la S-63 chiffrés conformément aux règles commerciales associées à la livraison de leurs données.

9.6 Processus de l'accord de licence

9.6.1 Déchiffrer le permis d'utilisateur

Cette procédure est réalisée par le fournisseur de données pour extraire le HW_ID (système identificateur unique) afin de produire les permis de cellule pour le système du client utilisateur de données. La structure du permis d'utilisateur est définie à la section 4.2.1. La procédure de déchiffrement du permis d'utilisateur est la suivante :

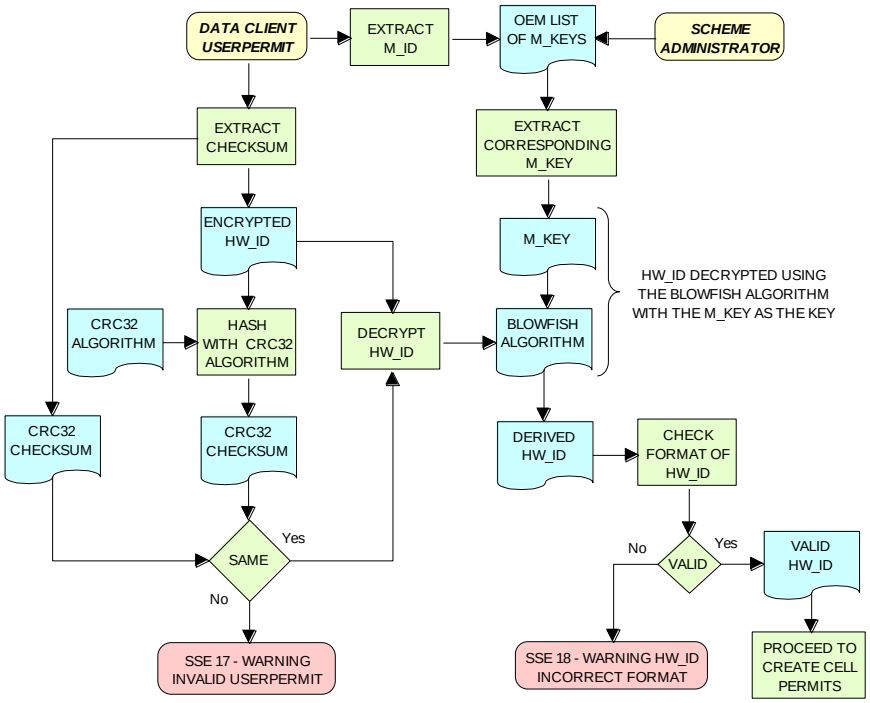
a) Extraire le M_ID (4 caractères hexadécimaux) du permis d'utilisateur.
b) Extraire la somme de contrôle (8 caractères hexadécimaux) du permis d'utilisateur.
c) Hacher le HW_ID chiffré (16 premiers caractères du permis d'utilisateur) en utilisant l'algorithme CRC32.
d) Comparer les résultats de 'b' et 'c'. S'ils sont identiques, le permis d'utilisateur est valide. Si les deux résultats diffèrent, le permis d'utilisateur n'est pas valide et le HW_ID ne peut être obtenu.
e) Si le permis d'utilisateur est valide, convertir le HW_ID chiffré à 8 octets.
f) Déchiffrer le HW_ID chiffré en utilisant l'algorithme Blowfish avec pour clé la M_KEY. Le résultat donnera le HW_ID.

Les fournisseurs de données doivent confirmer que toutes les HW_ID dérivées sont d'une longueur correcte comme défini dans la section 4.2.2.

Exemple:

Permis d'utilisateur	73871727080876A07E450C043031
M_KEY	3938373635 (ASCII)

Résultat de 'a'	3031	M_ID
Résultat de 'b'	7E450C04	Somme de contrôle extraite en hexadécimales
Entrée en 'c'	73871727080876A0	Les octets sont donnés à la fonction hachage en partant du premier octet gauche (c'est-à-dire 73, puis 87, puis 17 etc.)
Résultat de 'c'	7E450C04	Somme de contrôle de la HW_ID chiffrée extraite en caractères in hexadécimaux.
Résultat de 'f'	3132333438	HW_ID en caractères hexadécimaux



Data Server Process - Extract HW_ID from Userpermit

9.6.2 Créer le permis de cellule

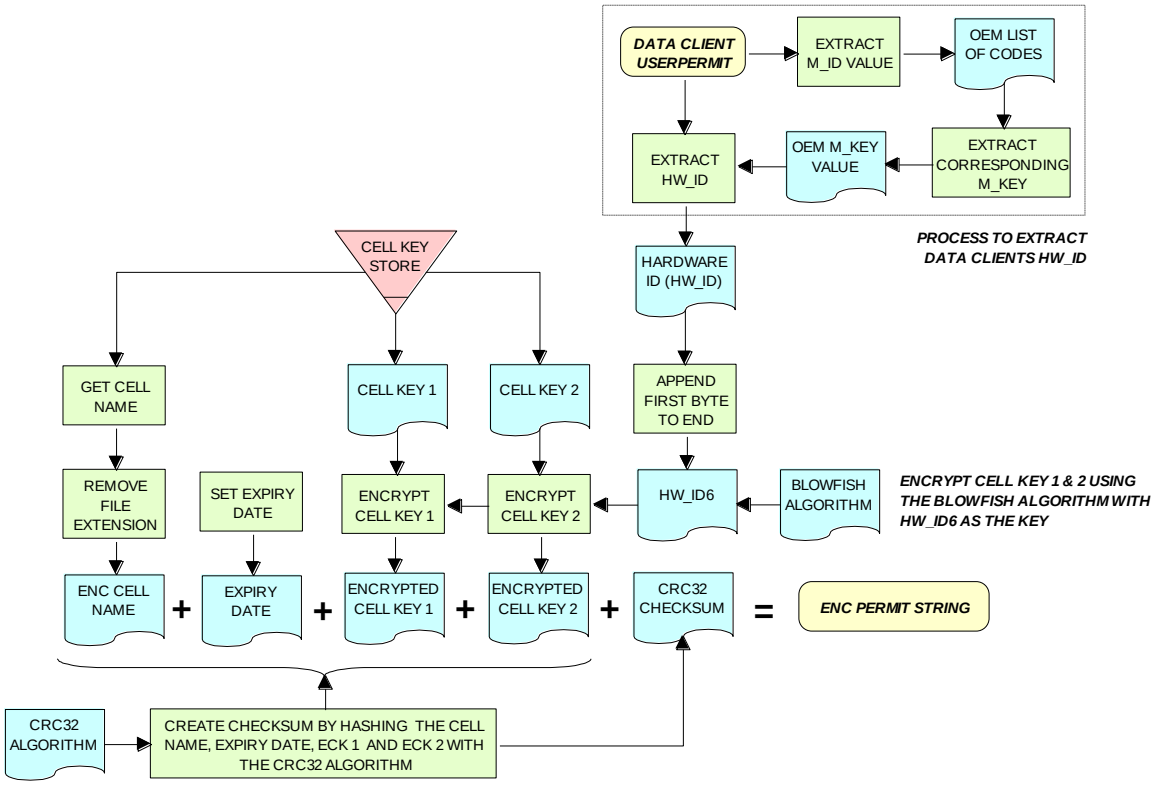
Le processus de création des permis de cellule est réalisé par les fournisseurs de données à la demande d'un client utilisateur de données. Le processus suivant est utilisé pour produire les permis de cellule selon la structure définie en section 4.3.

a) Enlever l'extention de fichier du nom de fichier ENC. Il reste 8 caractères et le nom de cellu_le du permis de cellule.
b) Ajouter la date d'expiration de la licence, en format YYYYMMDD, au nom de cellule obtenu en 'a'.
c) Ajouter le premier octet de HW_ID à la fin de HW_ID pour former un HW_ID de 6 octets (appelé HW_ID6). Ceci pour créer une clé de 48 octets pour chiffrer les clés de cellule.
d) Chiffrer la clé de cellule 1 en utilisant l'algorithme Blowfish avec HW_ID6 obtenu en 'c' comme clé au moyen de laquelle créer ECK1.
e) Convertir ECK1 à 16 caractères hexadécimaux. Tout caractère alphabétique doit être en majuscules.
f) Ajouter à 'b' le résultat de 'e'.
g) Chiffrer la clé de cellule 2 (CK2) en utilisant l'algorithme Blowfish avec HW_ID6 comme clé au moyen de laquelle créer ECK2.
h) Convertir ECK2 à 16 caractères hexadécimaux. Tout caractère alphabétique doit être en majuscules.
i) Ajouter à 'f' le résultat de 'h'.
j) Hacher le résultat de 'i' en utilisant l'algorithme CRC32. Il est à noter que le totall est haché après avoir été converti en une chaîne hxadécimale, comparée avec le permis d'utilisateur où le total est donné en données binaires brutes.
k) Chiffrer le total (résultat de 'j') en utilisant l'algorithme Blowfish avec HW_ID6 comme clé.
l) Convertir le résultat de 'k' en une chaîne de 16 caractères hexadécimaux. Tout caractère alphabétique doit être en majuscules. Ceci donne la somme de contrôle ENC.
m) Ajouter à 'i' le résultat de 'l'. Cela donne le permis de cellule.

Exemple:

HW_ID	3132333438	5 octets en hexadécimales
CK1	C1CB518E9C	5 octets en hexadécimales
CK2	421571CC66	5 octets en hexadécimales
Cell Name	NO4D0613.000	Nom de cellule S-57 avec extension de fichier
Expiry Date	20000830	Format YYYYMMDD

Résultat de 'a'	NO4D0613	Ceci est le nom de cellule
Résultat de 'b'	NO4D061320000830	Nom de cellule + date d'expiration
Résultat de 'c'	313233343831	HW_ID6 en hexadécimales.
Résultat de 'd' ou 'e'	BEB9BFE3C7C6CE68	ECK1 en hexadécimales
Résultat de 'f'	NO4D061320000830BEB9BFE3 C7C6CE68	Nom de cellule + date d'expiration + ECK1
Résultat de 'g' ou 'h'	B16411FD09F96982	ECK2 en hexadécimales
Résultat de 'i'	NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982	Nom de cellule + date d'expiration + ECK1 + ECK2
Entrée en 'j'	NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982	Les valeurs ASCII du résultat de 'i' (36 octets au total). Les octets sont donnés à la fonction de hachage en commençant par l'octet de gauche (c'est-à-dire xx, puis xx, puis xx etc).
Résultat de 'j'	780699093	CRC32 de 'j', nombre de 4 octets
Résultat de 'k'	8 octets non imprimables	CRC32 chiffrée
Résultat de 'l'	795C77B204F54D48	CRC32 chiffrée en hexadécimales
Permis de cellule	NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48	



Data Server Process - Create Cell Permit

9.6.3 Emission d'accord de licence ENC
Les fournisseurs de données émettront des accords de licence pour l'accès aux ENC chiffrées de la S-63 conformément aux règles commerciales associées à leur service de délivrance des données.

9.7 Procédures de sécurité relatives à l'assurance qualité – Fournisseur de données

9.7.1 Information sur le dispositif de protection des données
Le SA fournira des exemplaires de toutes les informations nécessaires au fournisseur de données pour exploiter le dispositif de protection des données.

9.7.2 Essais de conformité du système
Le fournisseur de données doit réaliser des essais de conformité interne de la mise en application du dispositif de protection, basés sur les descriptions fournies dans ce document et sur les données d'essais.

9.7.3 Stockage des M_ID et M_KEY
Une fois que le fournisseur de données a adhéré au dispositif, le SA doit lui fournir les informations spécifiques relatives aux M_ID et M_KEY pour tous les fabricants qui y participent. Le SA devra immédiatement informer les fournisseurs de données des amendements à la liste des M_ID et M_KEY au fur et à mesure que de nouveaux fabricants rejoignent le dispositif.

La réception de toutes les M_ID et M_KEY par le fournisseur de données doit être enregistrée de façon sécurisée dans un **Registre M_ID / M_KEY.**

9.7.4 Acceptation et contrôle du certificat numérique de SA (et clé publique)
Un fournisseur de données recevra la clé publique de SA en deux formats, en tant que certificat numérique X.509 et en tant que clé publique imprimable. Le fournisseur de données aura la capacité de charger le certificat numérique de SA et de comparer manuellement la clé publique et la clé publique imprimée. Le fournisseur de données devra accepter la clé publique de SA seulement une fois que ceci aura été fait. Ce processus s'applique à la clé publique originale de SA et à toutes les clés subséquemment émises par le SA.

Le fournisseur de données devra tenir à jour, dans un **Registre de clé publique de SA,** les enregistrements de clés publiques de SA qui ont été utilisées. Cet enregistrement contiendra un exemplaire de chaque clé ainsi que la date à laquelle celle-ci a été utilisée.

9.7.5 Création de clés de signature numérique (clés privées et clés publiques)
Le fournisseur de données aura la capacité de créer sa propre paire de clé privée et publique telle que décrite à la section 9.3.

La clé privée doit être stockée de façon sécurisée et son accès limité aux seules personnes qui ont besoin de la connaître. Le fournisseur de données créera une nouvelle paire de clé publique/privée et demandera au SA un nouveau certificat de fourniseur de données si sa clé privée est modifiée.

Le fournisseur de données devra créer une clé auto-signée (SSK) et l'envoyer au SA pour conversion en certificat de fournisseur de données. Dès réception, le SA contactera ce fournisseur de données pour confirmer que la SSK délivrée provient de la source indiquée.

9.7.6 Acceptation du certificat de fournisseur de données de la part du SA
Le fournisseur de données devra vérifier et stocker de façon sécurisée le certificat renvoyé par le SA en suivant le processus indiqué à la section 9.3.3.3.

9.7.7 Création de clés de cellule
Le fournisseur de données aura la capacité de créer et de gérer les clés de cellule, ainsi que défini à la section 9.5.1. Le fournisseur de données est responsable du stockage sécurisé des clés de cellule après qu'elles aient été créées.

9.7.8 Compression, Chiffrement et signature des données S-57
Le fournisseur de données aura la capacité de compresser, chiffrer et signer les informations ENC, comme défini aux sections 9.5.2, 9.5.3 et 9.5.4. L'accès au programme de signature doit être limité aux seules personnes autorisées à fournir les données.

9.7.9 Création de valeurs aléatoires

Pour signer les informations ENC, le fournisseur de données créera des valeurs aléatoires. Le fournisseur de données fera en sorte que la même valeur ne soit est pas utilisée pour deux signatures distinctes.

9.7.10 Création de permis de cellule

Le fournisseur de données doit pouvoir créer un permis de cellule pour un client utilisateur de donnée. Le fournisseur de donnéees doit émettre un nouveau permis de cellule pour ses clients utilisateurs de données lorsqu’une cellule ENC est chiffrée avec une clé de cellule différente (c’est-à-dire lorsqu’elle est émise en tant que nouvelle édition).

9.7.11 Déchiffrement des permis d’utilisateur

Le fournisseur de données doit pouvoir déchiffrer les permis d’utilisateur pour obtenir le HW_ID du client utilisateur de données. Le fournisseur de données a besoin du HW_ID pour créer un permis de cellule.

Page laissée en blanc intentionnellement

10. PROCESSUS RELATIFS AUX FABRICANTS ET AUX CLIENTS UTILISATEURS DE DONNEES

10.1 Clients utilisateurs de données

Les clients utilisateurs de données sont les utilisateurs des informations relatives aux ENC et ils reçoivent des informations protégées de la part des fournisseurs de données. Le fabricant est responsable du développement des applications du logiciel qui peuvent authentifier les signatures numériques ENC et déchiffrer les informations ENC, conformément aux procédures définies dans le dispositif de protection. Les navigateurs disposant de systèmes ECDIS/ECS sont des exemples de clients utilisateurs de données.

10.2 Les fabricants (OEM)

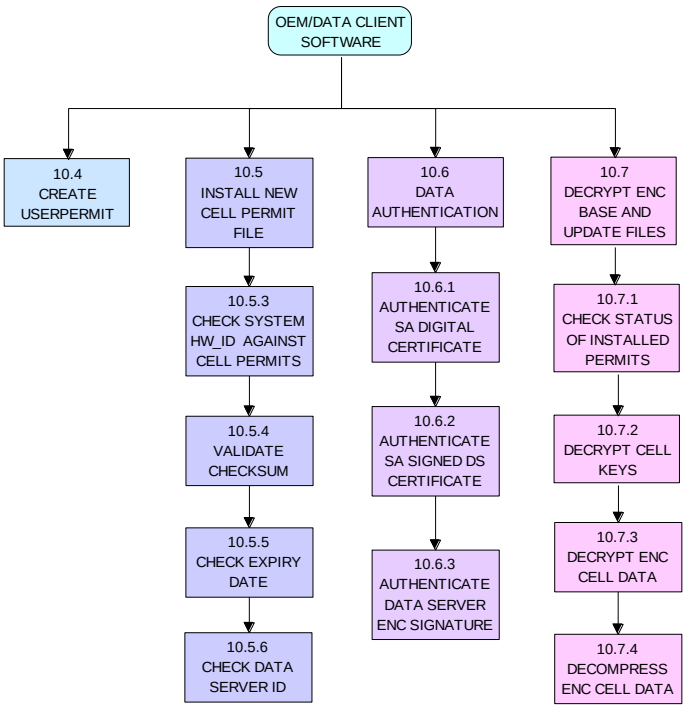
Les fabricants qui s'abonnent au dispositif de protection des données doivent construire des sous-programmes à l'appui du dispositif de protection des données. La norme S-63 contient des spécifications et des données d'essai pour la validation du logiciel d'application. Le SA fournit au fabricant un ensemble particulier de codes de fabricant (M_KEY et M_ID).

Le fabricant doit également fournir à l'intérieur de son système un mécanisme sécurisé pour identifier chaque installation d'utilisateur final. Le dispositif de protection des données nécessite que chaque installation ait un identificateur particulier de matériel (HW_ID). Les fournisseurs de données utilisent les informations M_KEY et HW_ID pour émettre des clés de cellule ENC chiffrées destinées à l'installation spécifique du client utilisateur de données. Chaque ENC est chiffrée avec une clé de cellule particulière, toutefois, le fait que le HW-ID du client utilisateur de données soit utilisé pour les chiffrer permet de s'assurer que les données ne peuvent pas être transférée entre plusieurs ECDIS provenant d'un même fabricant.

Il est demandé au fabricant de coopérer à la protection des informations ENC au sein des systèmes d'utilisateur final.

10.3 Processus relatifs au fabricant et au client utilisateur de données

Les responsabilités principales des fabricants autorisés et leurs logiciels d'applications sont décrites dans le diagramme ci-dessous. Chaque case du schéma établit des correspondances avec la section particulière où ces opérations sont détaillées.



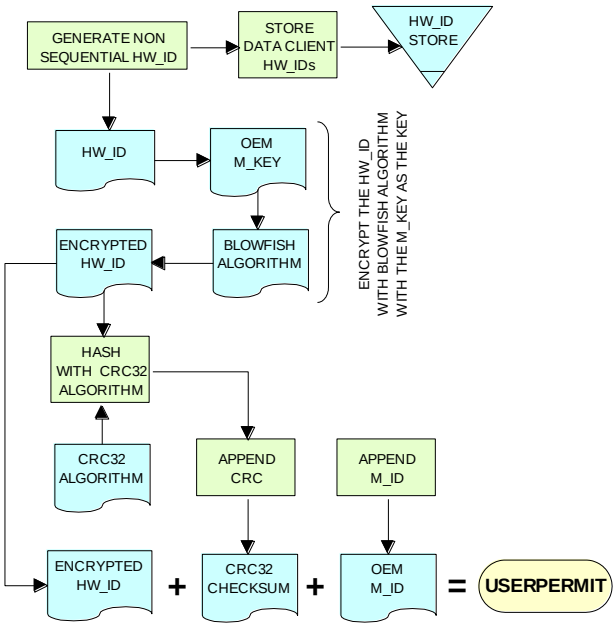
Main OEM/Data Client Processes

10.4 Création du permis d'utilisateur du client utilisateur de données

Cette procédure est mise en oeuvre par le fabricant du système (OEM) qui créé un permis d'utilisateur spécifique au client utilisateur de données. Ce permis est donné au client lorsqu'il acquiert un ECS/ECDIS. Ce permis d'utilisateur permet aux clients utilisateurs de données d'obtenir les permis de cellule des fournisseurs de données. Les permis de cellule sont générés au moyen d'un HW_ID chiffré qui se trouve dans le permis d'utilisateur. Le format et la structure du permis d'utilisateur sont définis à la section 4.2.

La procédure à suivre pour créer un permis d'utilisateur est la suivante :

a) Chiffrer le HW_ID en utilisant l'algorithme Blowfish avec M_KEY comme clé.
b) Convertir la valeur qui en résulte en une chaîne de 16 caractères hexadécimaux. Tout caractère alphabétique devra être en majuscules.
c) Hâcher les 16 caractères hexadécimaux en utilisant l'algorithme CRC32.
d) Convertir le résultat de 'c' en une chaîne de 8 caractères hexadécimaux. Tous les caractères alphabétiques devront être en majuscules. C'est la somme de contrôle.
e) Ajouter à 'b' le résultat de 'd'.
f) Convertir le M_ID en une chaîne de 4 caractères hexadécimaux. Tout caractère alphabétique devra être en majuscules.
g) Ajouter à 'e' le résultat de 'f' pour obtenir le permis d'utilisateur**.**



OEM - Create Userpermit

Exemple:

HW_ID	3132333438 (ASCII)
M_KEY	3938373635 (ASCII)
M_ID	3031 (ASCII)

Résultats prévus:

Entrée en 'a'	3132333438 et 3938373635	HW_ID et M_KEY en hexadécimales
Résultat de 'a'	8 octets	Non-imprimable.
Entrée en 'c'	73871727080876A0	Valeur hexadécimale de la chaîne ci-dessus. Les octets sont donnés à la fonction de hachage (somme de contrôle) en commençant par l'octet de gauche (c'est à dire 73, puis 87, puis 17 etc.)
Résultat de 'c'	7E450C04	Résultat CRC32 en hexadécimales
Résultat de 'e'	73871727080876A07E450C04	Résultat CRC32 ajouté à la HW_ID chiffrée.
Résultat de 'f'	3031	Résultat ajouté au HW_ID & CRC32 chiffrés
Résultat de 'e'	73871727080876A07E450C04	

10.5 Installation du permis de cellule pour ENC

Les nouveaux permis de cellule sont délivrés au système du client utilisateur de données sous forme d'un fichier intitulé PERMIT.TXT. La structure et le format de ce fichier sont indiqués à la section 4.3. Le système du client utilisateur de données doit pouvoir lire dans ce fichier et permettre de réaliser un certain nombre de contrôles. Chaque enregistrement de permis de cellule contient un identificateur du fournisseur de données qui permet au fabricant de gérer les permis et les données dans un environnement à fournisseurs multiples. Les sections suivantes mettent en évidence la manière dont ce fichier doit être géré ainsi que les contrôles qui doivent être réalisés lors de l'installation d'un nouveau fichier de permis.

10.5.1 Vérification du fichier de permis de cellule

Le système du client utilisateur de données doit contrôler en premier lieu qu'un fichier de permis de cellule à jour est prêt à être installé. Les clients utilisateurs de données doivent disposer d'une facilité permettant de rechercher un endroit spécifique sur le système où le fichier PERMIT.TXT peut être installé. Si un fichier texte autre que celui dénommé PERMIT.TXT est sélectionné le système devra adresser en retour un avertissement à savoir :

"SSE 11 – Fichier de permis de cellule introuvable »

10.5.2 Vérification du format de permis de cellule

Si un fichier PERMIT.TXT valide est localisé, le système doit ensuite contrôler que le format du fichier est correct comme indiqué dans la section 4.3. Dans le cas contraire, le client utilisateur de données doit informer l'utilisateur comme suit :

"SSE 12 – Format de permis de cellule incorrect".

10.5.3 Vérification du HW_ID

Le système du client utilisateur de données doit contrôler que le HW_ID codé dans le dispositif de sécurité de la clé de protection est semblable au HW_ID chiffré dans les permis de cellule. Si les valeurs sont identiques le système poursuivra les contrôles ci-dessous, dans le cas contraire, un message d'erreur doit être retourné comme suit :

"SSE 19 –Permis non valides pour ce système. Veuillez contacter votre fournisseur de données pour obtenir les permis corrects ".

10.5.4 Vérification du total de contrôle du permis de cellule

Cette procédure est normalement suivie par le système du client utilisateur de données et comprend les étapes suivantes :

a) Extraire du permis de cellule les 16 derniers caractères hexadécimaux (somme de contrôle ENC).
b) Convertir ces 16 caractères hexadécimaux en 8 octets.
c) Hacher le reste du permis de cellule tel qu'après 'a' en utilisant l'algorithme CRC32.
d) Ajouter le premier octet de HW_ID à la fin de HW_ID pour former un HW_ID de 6 octets (appelé HW_ID6).
e) Chiffrer la sortie de 'c'(hachée) en utilisant l'algorithme Blowfish avec HW_ID6 comme clé.
f) Comparer la sortie de 'e' avec la sortie de 'b'. Si elles sont identiques, le permis de cellule est valide. Si elles sont différentes, le permis de cellule est corrompu et ne peut être utilisé.

Par exemple :

HW_ID	3132333438	sous forme hexadécimale
Permis de cellule	NO4D061320000830BEB9BFE3C7C6CE68B16 411FD09F96982795C77B204F54D48	exemple de permis de cellule

Résultat de 'a'	795C77B204F54D48	sous forme hexadécimale
Résultat de 'b'	8 octets non imprimables	CRC32 chiffré
Entrée en 'c'	NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982	Permis de cellule après suppression du CRC32 chiffré de 16 caractères hexadécimaux. Les octets sont donnés à la fonction de hachage en commençant par l'octet de gauche (c'est à dire xx, puis xx, puis xx, etc.
Résultat de 'c'	780699093	CRC32 de 4 octets du permis de cellule après suppression du CRC32 de 16 caractères hexadécimaux chiffrés.
Résultat de 'd'	313233343831	Ceci est le HW_ID6
Résultat de 'e'	8 octets non imprimables	CRC32 chiffré

Si la valeur du CRC32 calculée n'est pas la même que la valeur contenue dans le permis de cellule le système doit informer le client utilisateur de données comme suit:

"SSE 13 Permis de cellule invalide (somme de contrôle incorrecte)

Le système ne doit pas installer de permis invalides.

10.5.5 Vérification de la date d'expiration du permis de cellule

Lorsqu'on installe un nouveau fichier PERMIT.TXT, le système du client utilisateur de données doit vérifier que les permis installés ne sont pas arrivés à expiration. Le système doit vérifier la date d'expiration de chaque permis par rapport à la date du système (horloge de l'ordinateur) et si possible l'heure du signal du receveur GPS. Si les permis sont arrivés à expiration le message suivant devrait être affiché

"SSE 15 – Expiration de l'abonnement. Veuillez contacter votre fournisseur de données pour renouveler la licence d'abonnement".

NOTE: Le système peut installer des permis expirés/valides mais toutes les cellules qui sont visualisées par la suite sur l'écran de visualisation dans ces conditions **DOIVENT** afficher un avertissement permanent à l'attention de l'utilisateur, à savoir:

"SSE 25 - Le permis ENC a expiré pour cette cellule. Cette cellule peut être périmée et ne DOIT PAS être utilisée pour la NAVIGATION. »

Voir section 10.7.1.1 pour la vérification de la date d'expiration au moment du chargement.

Si la date d'expiration du permis est en avance sur l'horloge de l'ordinateur/le signal GPS alors un contrôle supplémentaire devra être fait pour voir combien de temps la licence d'abonnement doit durer. Si c'est 30 jours ou moins alors le système devra produire un avertissement informant le client utilisateur de données comme suit :

"SSE 20 – L'abonnement expirera dans moins de 30 jours. Veuillez contacter votre fournisseur de données afin de renouveler la licence d'abonnement."

Le client utilisateur de données peut ensuite prendre les mesures nécessaires pour renouveler la licence avant qu'elle n'expire. Le système devrait alors procéder à l'installation des permis. Si le permis a plus de 30 jours avant expiration, il peut être installé sans avertissement.

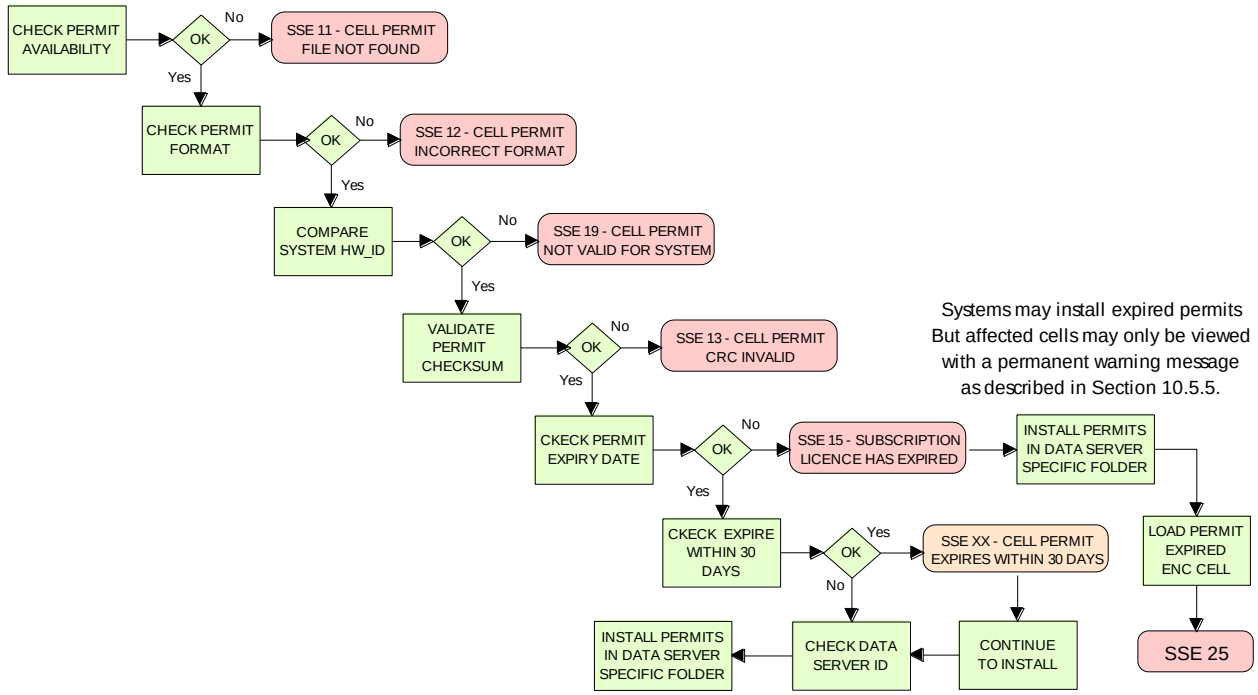
10.5.6 Vérification de l'identificateur du fournisseur de données

Le dispositif de protection des données de la S-63 tient compte d'un environnement à fournisseurs multiples, ce qui signifie que les clients utilisateurs de données peuvent obtenir des licences à partir de plusieurs fournisseurs de données. Dans plusieurs cas, les clients utilisateurs de données peuvent obtenir des données ENC provenant de fournisseurs multiples, comme suit:

- Doubles de cellules autorisées provenant de différents fournisseurs de données
- Changement d'un fournisseur de données à l'autre.

Il est important que ces cas puissent être grés par les systèmes de client utilisateur de données. Chaque enregistrement de permis contient un champ d'identification du fournisseur de données (voir section 4.3.3). Ce champ, s'il est rempli, contient un identificateur à deux caractères alphanumériques particulier à chaque fournisseur de données attribué par le SA. Etant donné que les permis de cellule émis par un fournisseur de données ne déchiffreront pas nécessairement les ENC fournies par un autre, il est important de maintenir un lien entre les permis de cellule et les ENC chiffrées. Les fabricants de cellule devraient faire en sorte que leurs systèmes soient capables de maintenir ces associations, par exemple en créant des dossiers spécifiques de fournisseur de données où les permis seraient stockés.

L'identificateur du fournisseur de données pour les ensembles de données d'échange chiffrées pour ENC est contenu dans le fichier SERIAL.ENC (voir section 6.3.1). Il est identique à celui contenu dans l'enregistrement de permis de cellule.



OEM System - Install & Validate Cell Permit

10.6 Vérification de l'authentification et de l'intégrité des ENC

Les systèmes des fabricants doivent être capables d'authentifier la source des données ENC chiffrées et de valider leur intégrité. Ceci est obtenu des deux manières suivantes:

- En authentifiant la signature du SA détenue en tant que partie intégrante du certificat de fournisseur de données qui forme une partie du fichier de signature ENC.
- En validant la signature du fournisseur de données ENC (correspondant aux données de cellule pour ENC) dans le fichier de signature ENC.

Les fabricants et les clients utilisateurs de données doivent en premier lieu confirmer que le certificat de SA (qu'il soit au format X509 ou autre) installé sur l'ECS/ECDIS est correct et actuel. Ceci est traité dans la section 10.6.1 ci-dessous.

10.6.1 Authentifier/vérifier le certificat numérique du SA

Cette procédure est réalisée par les fabricants ou les clients utilisateurs de données pour vérifier que la clé publique installée dans l'ECS/ECDIS est correcte et à jour en ce qui concerne le dispositif de protection des données de l'OHI (S-63). C'est cette clé publique du SA qui est utilisée pour authentifier le certificat de fournisseur de données signé par le SA fourni aux fournisseurs de données dans le cadre du fichier de signature ENC. La procédure est la suivante :

Comparer manuellement la clé publique de SA contenue dans le certificat numérique de SA installée indépendamment avec une copie imprimable disponible à partir du site web de l'OHI (http://www.iho.int). Si la vérification ci-dessus échoue, le système n'acceptera pas le certificat numérique de données SA. Dans le cas contraire, le certificat numérique du SA est valide et la clé publique de fournisseur de données qu'il contient peut être utilisée pour authentifier le certificat de fournisseur de données du SA, détenu dans le cadre du fichier de signature ENC.

NOTE: Le client utilisateur de données doit pouvoir accéder au certificat installé à partir de l'application.

10.6.1.1 Vérification manuelle de la clé publique de SA

La clé publique de SA peut être obtenue à partir du site web de l'OHI comme suit :

www.iho.int → Normes et Publications → Téléchargement → S-63 → S-63 SA Certificate

La page web suivante sera affichée:

« ***S-63 CERTIFICATS NUMERIQUES***
Les certificats numériques sont des fichiers qui lient une clé publique spécifique et d'autres informations à un particulier ou une organisation. La norme S-63 utilise une chaine à deux niveaux de certificats pour exploiter le dispositif de protection des données.

Le BHI est l'Administrateur du dispositif et il a émis le certificat numérique de base à utiliser au sein du dispositif de protection. Le certificat du utilisé par le BHI sera un certificat auto-signé. Il est disponible à la fois en tant que fichier ***IHO.CRT*** *compatible x-509 et en tant que fichier texte* ***Scheme Administrator Public Key.txt.*** *Ces deux fichiers sont contenus dans un fichier compressé de certificat de* ***SA Certificate.***

L'Administrateur du dispositif émettra des certificats de fournisseur de données à tous les fournisseurs de données participant au dispositif de protection. Le certificat de fournisseur de données contient une clé publique de fournisseur de données et la signature par le SA de cette clé. Etant donné que seul le SA peut émettre des certificats de fournisseurs de données, la chaîne de confiance peut être établie en authentifiant la signature du SA sur la clé publique du fournisseur de données.

Le dispositif de protection nécessite que la clé publique de SA soit installée sur les systèmes de l'utilisateur final par tous les utilisateurs du dispositif de protection. Le certificat de fournisseur de données est contenu au sein de chaque fichier de signature et la clé publique de fournisseur de données peut être fiable si le certificat de SA est valide. L'installation du certificat de SA (et la clé publique qu'il contient) devrait être menée à bien en tant qu'opération indépendante, séparée et faire l'objet de procédures opérationnelles soigneusement controlées. »

Dans le second paragraphe ci-dessus, un clic sur le lien ***"SA Certificate"*** *et un dialogue* ***"File Download"*** *sont visualisés ce qui donnera à l'utilisateur l'option* ***d'"ouvir"*** *ou de* ***"sauver"*** *le fichier compressé intitulé* ***"S-63_SA_Certificate.zip".*** *Ce fichier contient deux fichiers à savoir:*

1. IHO.CRT (Le X509 Certificat)

Un dialogue ***"Certificate"*** est visualisé lorsqu'on ouvre ce fichier, lorsqu'on sélectionne l'onglet ***"Details"*** et surligne ***"Public Key"*** la clé publique de l'OHI apparaît. L'exemple ci-dessous représente la clé publique de l'OHI au moment où ce document a été publié. Veuillez noter que les 6 premiers caractères [024100] représentent les paramètres du certificat et peuvent être soit positifs [0240] soit négatifs [024100].

```
0241 0096 3F14 E32B A537 2928 F24F 15B0 730C
49D3 1B28 E5C7 6410 0256 4DB9 5995 B15C F880
0ED5 4E35 4867 B82B B959 7B15 8269 E079 F0C4
F492 6B17 761C C89E B77C 9B7E F8
```

Cette chaîne de caractères (moins les paramètres du certificat) devrait être comparée au certificat installé afin de confirmer qu'elles sont semblables. Si cela est le cas, alors le certificat est authentifier, dans le cas contraire, il devrait être rejeté.

2. Fichier Public Key.txt de SA

Les paramètres de clé publique de SA suivants s'affichent à l'ouverture de ce fichier.

```
// BIG p
FCA6 82CE 8E12 CABA 26EF CCF7 110E 526D B078 B05E DECB CD1E B4A2 08F3 AE16 17AE
01F3 5B91 A47E 6DF6 3413 C5E1 2ED0 899B CD13 2ACD 50D9 9151 BDC4 3EE7 3759 2E17.
// BIG q
962E DDCC 369C BA8E BB26 0EE6 B6A1 26D9 346E 38C5.
// BIG g
6784 71B2 7A9C F44E E91A 49C5 147D B1A9 AAF2 44F0 5A43 4D64 8693 1D2D 1427 1B9E
3503 0B71 FD73 DA17 9069 B32E 2935 630E 1C20 6235 4D0D A20A 6C41 6E50 BE79 4CA4.
// BIG y
963F 14E3 2BA5 3729 28F2 4F15 B073 0C49 D31B 28E5 C764 1002 564D B959 95B1 5CF8
800E D54E 3548 67B8 2BB9 597B 1582 69E0 79F0 C4F4 926B 1776 1CC8 9EB7 7C9B 7EF8.
```

Si ce fichier est utilisé pour l'authentification, il devrait être vérifié par rapport au certificat installé ou à la clé publique. S'il est vérifié par rapport au certificat installé alors seulement la chaîne *"BIG y"* devrait être vérifiée pour voir s'il s'agit de la même clé. S'il est vérifié par raport au fichier de clé publique alors seulement tous les paramètres devraient être vérifiés pour voir s'il s'agit de la même clé. Dans les deux cas, si le fichier est correct, la clé publique est alors authentifiée, dans le cas contraire, doit être rejeté.

10.6.2 Authentifier le certificat de fournisseur de données signé par le SA

Cette procédure est réalisée par le système du client utilisateur de données pour authentifier le certificat de fournisseur de données signé par le SA, stocké en tant qu'élément du fichier de signature ENC par rapport à la clé publique de SA installée. Ce processus est réalisé avant que la clé publique du fournisseur de données ne soit extraite pour authentifier la signature ENC. Voir section 5.3.2. pour la structure des paires signature/certificat dans un fichier de signature.

Avant d'entamer le processus d'authentification, le système doit d'abord vérifier la disponibilité, le format et l'état du certificat ou de la clé publique installé (e) sur le système. En cas de problème, celui-ci devrait être rapporté au client utilisateur de données de façon claire, comme suit :

1. Certificat de SA ou clé publique indisponible dans le système (SSE 05 et fin du processus)
2. Format de certificat de SA ou de clé publique incorrect (SSE 08 et fin du processus).
3. Certificat de SA périmé (SSE 22 et fin du processus).

La procédure d'authentification est soulignée ci-dessous :

a. Extraire le fichier de signature ENC.
b. Eliminer la première partie de la signature (par exemple les deux premières chaînes et leurs en-têtes attenants. Ceci représente la signature du fournisseur de données des données ENC. Ceci donne le certificat de fournisseur de données signé par le SA.
c. Extraire la partie de la signature restante (par exemple les deux premières chaînes de données et leurs en-têtes attenants du reste du fichier obtenu en b). Ceci donne un fichier de clé publique.
d. Hacher le fichier de clé publique (obtenu en 'c') en utilisant l'algorithme ***SHA-1*** [3]. Tous les octets à l'intérieur du fichier doivent être hachés.
e. Vérifier la partie de la signature (celle supprimée en 'c' ci-dessus) en la passant (la signature), avec le fichier de clé publique de SA (la clé) et le hachage du fichier de clé publique (tel qu'obtenu en « d » au travers du **DSA** [2]. Ceci fournit en retour l'état (correct ou incorrect).

S'il est incorrect, le système doit terminer le processus et renvoyer le message suivant d'avertissement.

"SSE 06 – Le certificat de fournisseur de données signé par le SA n'est pas valide. Le SA peut avoir émis une nouvelle clé publique ou l'ENC peut provenir d'un autre service. Une nouvelle clé publique de SA peut être obtenue à partir du site web de l'OHI ou bien de votre fournisseur de données".

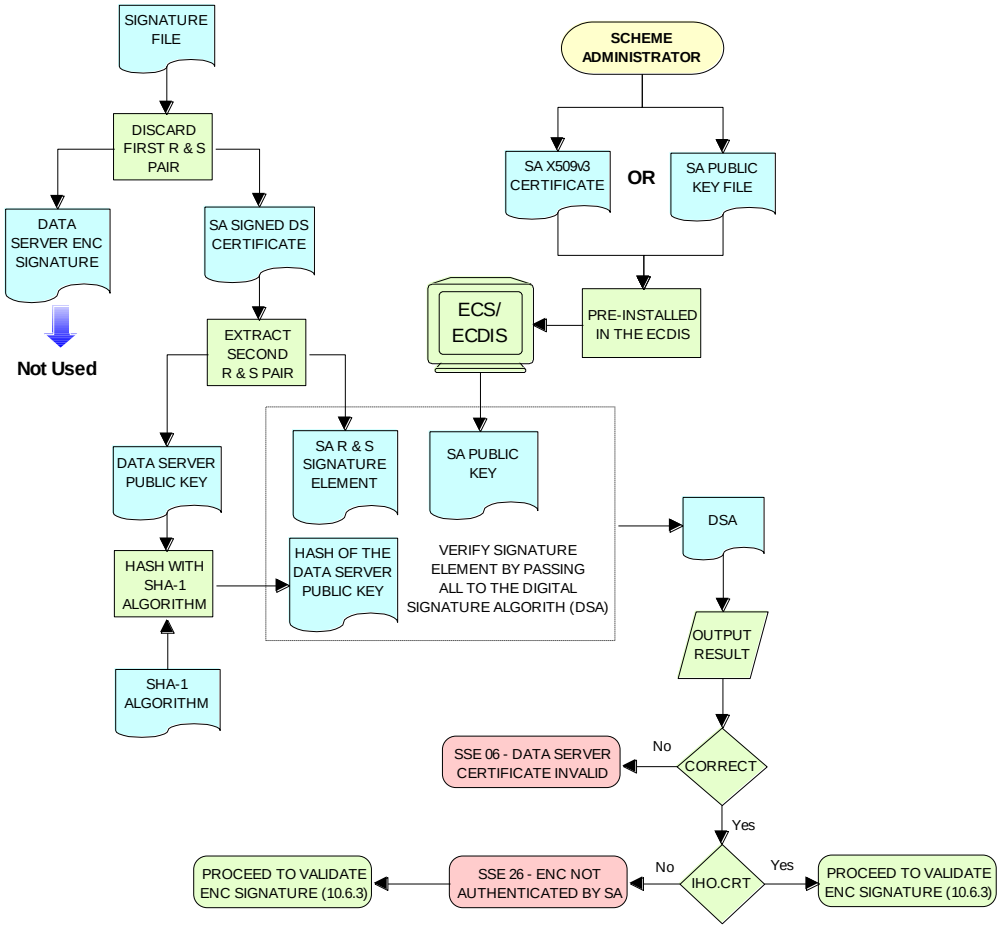
10.6.2.1 Authentification par rapport au certificat de fournisseur de données non signé par le SA

Il peut y avoir des cas où plus d'un certificat ou d'une clé publique sont stockés sur le système du client utilisateur de données. Ceci peut arriver particulièrement au cours de la transition vers l'utilisation correcte de l'usage du dispositif de la S-63. En conséquence, une vérification est nécessaire pour faire en sorte qu'on authentifie correctement le certificat de fournisseur de données à l'aide des fichiers IHO.CRT ou IHO.PUB installé sur le système du client utilisateur de données.

Si le certificat de fournisseur de données est authentifié par rapport à autre chose que les fichiers IHO.CRT ou IHO.PUB stocké sur le système du client utilisateur de données, alors un message d'avertissement DOIT être affiché comme suit :

"SSE 26 - "Cette ENC n'est pas authentifiée par l'OHI agissant en tant qu'Administrateur du dispositif"

Si ce message s'affiche le client utilisateur de données devrait encore continuer jusqu'au prochain stade de l'authentification de la signature ENC et du déchiffrement.



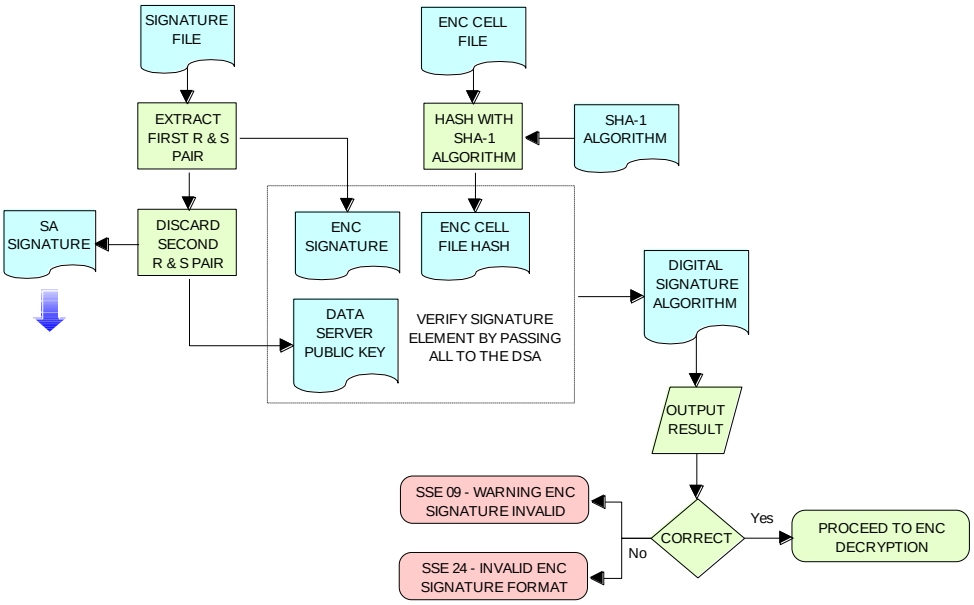
Authenticate SA Signed Data Server Certificate

10.6.3 Authentifier le fichier de cellule ENC

Cette procédure est réalisée par les systèmes des clients utilisateurs de données pour valider la signature ENC (détenue dans le fichier de signature ENC) correspondant à un fichier de cellule ENC spécifique. Le client utilisateur de données doit avoir déjà effectué les procédures en vue d'authentifier le certificat numérique de SA (section 10.6.1) et le certificat de fournisseur de données (section 10.6.2). La procédure d'authentification du fichier de cellule ENC est la suivante :

a) Extraire le fichier de signature ENC uniquement lié au fichier de cellule ENC.
b) Extraire la première partie de la signature (par exemple les deux premières chaînes de données et les en-têtes attenants).Ceci donne le certificat.
c) Eliminer la partie de la signature restante (par exemple les deux premières chaînes de données et leurs en-têtes attenants du reste du fichier. Ceci donne le fichier de clé publique.
d) Hacher le fichier de cellule ENC associé en utilisant l'algorithme *SHA-1* [3]. Tous les octets à l'intérieur du fichier doivent être hachés.
e) Vérifier la partie de la signature (telle qu'extraite en 'b' ci-dessus) en la passant (la signature), la clé publique – telle qu'en 'c' ci-dessus (la clé) et le hachage du fichier de cellule ENC, tel qu'obtenu en 'd' ci-dessus, au travers du *DSA* [2]. Ceci fournit en retour un état (correct ou incorrect).

Si la signature ENC n'est pas authentifiée correctement, le client fournisseur de données ne déchiffrera pas l'ENC parce que son origine ne pourra pas être vérifiée. Si l'ENC est authentifiée correctement, l'ENC peut être déchiffrée en toute sécurité.



Authenticate ENC Cell File - Validate ENC Signature

10.7 Déchiffrage des fichiers de cellule de base ENC et de mises à jour

Avant de déchiffrer les nouveaux fichiers de cellules de base et de mises à jour, le système devrait d'abord vérifier l'état de l'abonnement des permis de cellule installés. Ce processus sert à déterminer si le client utilisateur de données est autorisé à recevoir et à installer de nouvelles données ENC. Il cherche également à émettre des messages d'avertissement adéquat au client utilisateur de données avant la date d'expiration du permis.

10.7.1 Vérifier l'état de l'abonnement des permis installés

La Section 10.5 a identifié les processus et les vérifications qui sont réalisés par le système du client utilisateur de données lors de l'installation des permis de cellule. Cette section détermine combien de permis de cellule sont gérés par un système de client utilisateur de données une fois qu'il est installé. Il est également destiné à donner aux clients utilisateurs de données des avertissements anticipés pour les permis d'abonnement qui arrivent à expiration, particulièrement lorsque les données ENC sont utilisées pour la navigation.

10.7.1.1 Vérifier si l'abonnement est arrivé à expiration dans un permis de cellule – Avertissement requis

Ce contrôle est réalisé sur les nouvelles cellules de base ENC et les fichiers de mise à jour avant le déchiffrement. Ce contrôle est nécessaire pour informer le client utilisateur de données que la souscription est arrivée à son terme mais que les cellules ENC supplémentaires, cellules de base/mises à jour sont disponibles. L'avertissement ne s'applique qu'aux autorisations d'abonnement et pas aux autorisations d'achat spécifique, voir section 4.3.3. La procédure est précisée dans le diagramme ci-dessous et la description point par point suivante :

a) Extraire la date d'expiration du permis de cellule ENC chargé correspondant au fichier ENC à déchiffrer.

b) Extraire les dates d'émission du fichier ENC (cellules de base et dernières mises à jour) si elles sont disponibles[12]) à déchiffrer à partir du fichier PRODUCTS.TXT file. Elles se trouvent dans le deuxième (date d'émission du produit) et quatrième (date d'émission de la dernière mise à jour) champ de l'enregistrement de cellule correspondant à la cellule qui est déchiffrée.

c) Si deux dates (dans les champs deux et quatre) sont obtenues en b), seulement la dernière date[13] devrait être utilisée au moment du contrôle de la date d'expiration.

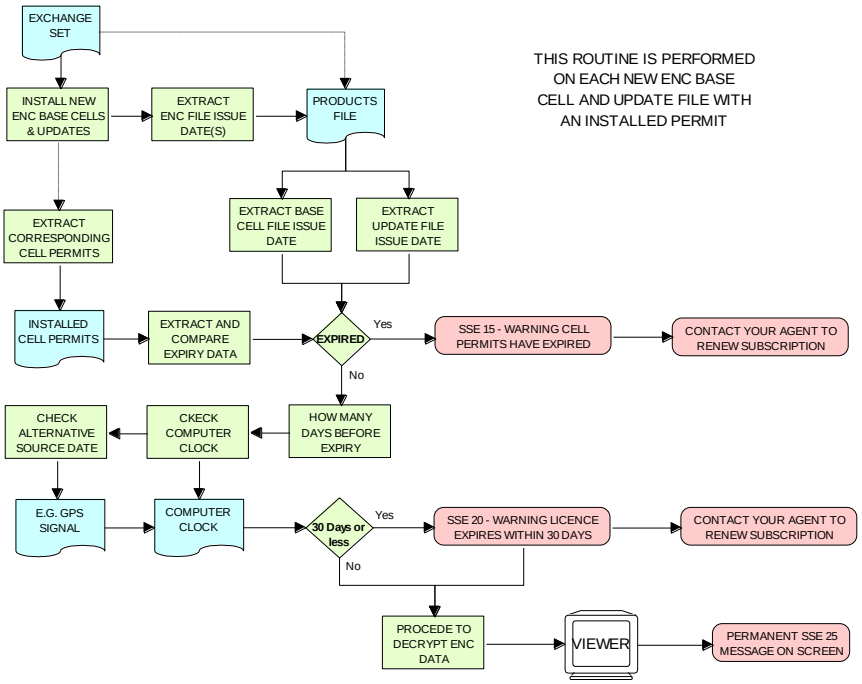
d) Si la date d'émission de la cellule de base ou de la mise à jour obtenue en b) et c) est antérieure (plus récente) à la date d'expiration du permis obtenu en a) on considère que les permis sont arrivés à expiration. L'avertissement suivant devra être affiché :

"SSE 15 – Le service d'abonnement est arrivé à expiration. Veuillez contacter votre distributeur pour le renouvellement de l'abonnement."

L'application peut **installer des permis ENC arrivés à expiration** mais doit afficher l'avertissement **"*SSE 15"*** ci-dessus. Elle peut également déchiffrer tout fichiers ENC (cellules de base et mises à jour) avant la date d'expiration s'ils sont antérieurs à la date d'expiration des permis. Ceci peut être réalisé en utilisant la date d'émission [ISDT] contenue dans le champ CATD-COMT au moment de l'importation. Aucune cellule de base ou mise à jour ne devrait être importée si la date d'émission [ISDT] est postérieure à la date d'expiration des permis de cellule installés. L'application doit également afficher un avertissement permanent lorsque les cellules ayant des permis arrivés à expiration sont affichés dans le système du client utilisateur de données voir section 10.8.1.

[12] Si aucune mise à jour n'a été émise pour une cellule il n'y aura pas d'information disponible.

[13] Le champ "Date d'émission de la dernière mise à jour", s'il est rempli, ne se trouvera pas toujours avant le champ "Date d'émission du produit", par exemple dans le cas des réémissions.



Process to Check Subscription Status before Decryption

10.7.1.2 Vérification de l'état de l'abonnement– Avertissement requis 30 jours à l'avance

Cette vérification doit être réalisée chaque fois que de nouveaux fichiers ENC (fichiers de base ou mises à jour) sont installés et elle est exigée afin d'informer le client utilisateur de données de l'état de la licence d'abonnement avant qu'elle n'expire. Le but est d'assurer que le client utilisateur de données ait le temps de renouveler son abonnement et d'obtenir un permis de cellule mis à jour à partir du serveur de données. L'avertissement est applicable seulement pour les licences d'abonnement et il ne doit pas être utilisé pour les licences d'achat spécifique, réf. Section 4.3.3. La procédure est la suivante:

a) Obtenir la date du système et, si celle-ci est disponible, toutes autres sources fiables relatives au temps, par exemple signal GPS.
b) Obtenir la date d'expiration de l'abonnement à partir du fichier de permis de cellule.
c) Comparer la date du système en "a" et la date d'expiration de l'abonnement en "b".
d) S'il y a 30 jours ou plus avant expiration de l'abonnement, le système peut opérer sans autre notification à l'utilisateur.
e) S'il y a moins de *30 jours* avant expiration de l'abonnement, le système peut être en mesure de déchiffrer et décompresser les nouvelles informations émises au cours de la durée de l'abonnement. Le système peut émettre un message d'avertissement à l'utilisateur du type:

"SSE 20 – Le service d'abonnement expire dans moins de 30 jours. Veuillez contacter votre fournisseur de données pour le renouvellement de votre abonnement.

10.7.2 Déchiffrer les clés de cellule dans un permis de cellule

Cette procédure est réalisée par le système du client utilisateur de données après l'authentification réussie du fichier de signature ENC. Le processus de déchiffrement commence avec l'extraction des clés de cellule requises afin de déchiffrer les ENC et se décompose comme suit :

a) Ajouter le premier octet de HW_ID du client utilisateur de données à la fin de HW_ID pour former un HW_ID de 6 octets (appelée HW_ID6).
b) Extraire ECK1 du permis de cellule et le convertir d'une chaîne de 16 caractères hexadécimaux en 8 octets.
c) Déchiffrer l'ECK1 converti (sortie de 'b') en utilisant l'algorithme Blowfish avec le HW_ID6 comme clé. Ceci donnera la clé de cellule CK1.

d) Extraire l'ECK2 du permis de cellule et le convertir d'une chaîne de 16 caractères hexadécimaux en 8 octets.
e) Déchiffrer l'ECK2 converti (sortie de "d") en utilisant l'algorithme Blowfish avec HW_ID6 en tant que clé. Ceci donnera la clé de cellule CK2**.**

Exemple:

HW_ID	3132333438	en hexadécimales
Permis de cellule	NO4D061320000830BEB9BFE3C7C6CE68 B16411FD09F96982795C77B204F54D48	Exemple de permis de cellule

Sortie de 'a'	313233343831	HW_ID6
Sortie de 'b'	8 octets non imprimables	ECK1 chiffré
Sortie de 'c'	C1CB518E9C	Clé de cellule 1 (hex)
Sortie de 'd'	8 octets non imprimables	ECK2 chiffré
Sortie de 'e'	421571CC66	Clé de cellule 2 (hex)

Il est à noter que les clés de cellule non chiffrées sont d'une longueur de 5 octets même si les clés de cellule chiffrées sont d'une longueur de 8 octets. La raison en est que l'algorithme Blowfish complète les clés de cellule pour obtenir une longueur de 8 octets lorsqu'il les chiffre et qu'il les ramène à une longueur de 5 octets lorsqu'il les déchiffre.

10.7.3 Déchiffrer le fichier de cellule de base ou de mise à jour pour ENC

Cette procédure est réalisée par le système du client utilisateur de données et est menée à bien comme indiqué dans le diagramme (pour les sections 10.7.2 et 10.7.3 et le guide étape par étape ci-dessous.[14]:

a) Déchiffrer le fichier ENC en utilisant l'algorithme Blowfish avec CK1 comme clé de déchiffrement.[15].
b) Décompresser le fichier ENC. Si la décompression est réussie, le fichier ENC est déchiffré et prêt pour l'importation.
c) Si la décompression n'est pas réussie, déchiffrer le fichier ENC en utilisant l'algorithme Blowfish avec CK2 comme clé de déchiffrement.
d) Décompresser le fichier ENC. Si la décompression est réussie, le fichier ENC est déchiffrer et prêt à être utilisé.
e) Si la décompression n'est pas réussie en "b" et "d", cela signifie que le permis de cellule ne contient aucune clé de cellule valide. Le système devrait renvoyer un message d'avertissement et informer le client utilisateur de données qu'un nouveau permis de cellule devrait être obtenu à partir du fournisseur de données.

"SSE 21 –Le déchiffrement a échoué, pas de permis de cellule valide trouvé. Les permis peuvent être utilisé pour un autre système ou de nouveaux permis peuvent être demandés, veuillez contacter votre fournisseur pour obtenir une nouvelle licence.

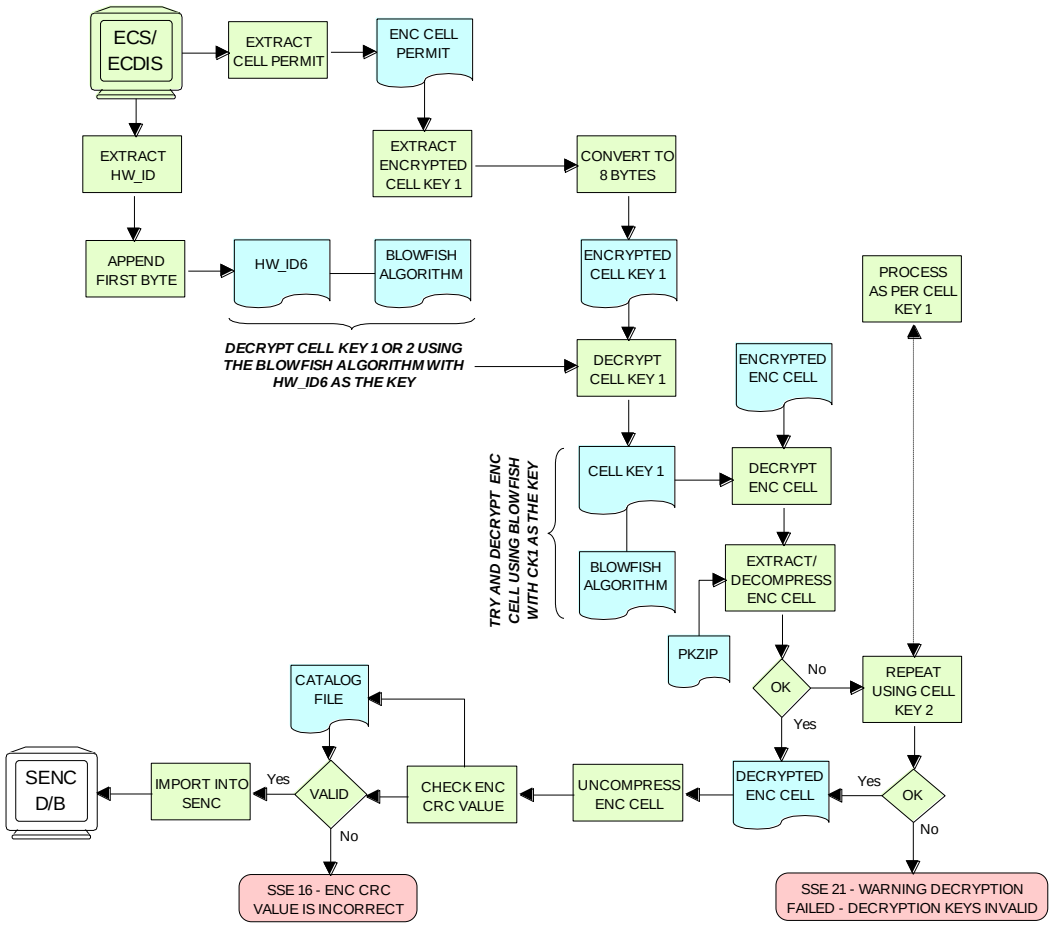
10.7.4 Décompresser le fichier ENC (cellule de base ou mise à jour)

Cette procédure est réalisée par le client utilisateur de données sur les fichiers ENC déchiffrés. La procédure est la suivante :

Décompresser le fichier ENC en utilisant la norme ZIP [6] pour créer un fichier entièrement conforme à la spécification de produit pour ENC de l'édition 3.1 de la S-57.

---

[14] OEMs should note that there is no requirement to check the edition date against the permit or words to this effect.
[15] Rather than decrypting and decompressing the entire ENC file the data client can check that the decrypted header information is compliant with the ZIP standard [6].



Decrypt & Uncompress ENC Base Cell and Update Files

NOTE: La valeur CRC de l'ENC [1] est toujours calculée sur les informations ENC déchiffrées. L'application doit confirmer que le déchiffrement et la décompression sont réussis en menant le contrôle CRC sur toutes les informations ENC.

10.8 Avertissements permanents du client utilisateur de données

Le client utilisateur de données réalise déjà des contrôles lorsqu'il charge les permis et les fichiers de données ENC pour valider leur conformité avec la norme. Cependant, toutes les erreurs ou les messages d'avertissements en résultant ne sont pas toujours transmis par l'ECDIS lorsque celui-ci est utilisé (planification de la route ou navigation, par exemple). Il est possible, dans le cadre du dispositif actuel de protection des données, d'utiliser des ENC périmées sans que l'utilisateur ne le sache. Le but de cette section est d'identifier les messages qui devraient être affichés de façon permanente par le client utilisateur de données en cours d'utilisation.

Le client utilisateur de données doit afficher des messages d'avertissement permanents à l'écran, lorsqu'on peut déterminer que les informations ENC contenues dans le SENC sont ou peuvent être périmées. Le client utilisateur de données doit effectuer les contrôles suivants lors de la visualisation d'une cellule sur l'ECDIS:

- Les permis ENC installés sont-ils arrivés à expiration?
- Les données SENC installées sont-elles périmées par rapport au dernier fichier PRODUCTS.TXT installé?

10.8.1 Permis ENC étant arrivé à expiration

Le client utilisateur de données doit vérifier l'état du permis ENC installé lorsqu'il visualise une cellule ENC spécifique. Si le permis a expiré, l'ECDIS doit afficher un avertissement permanent informant l'utilisateur que cette cellule ENC risque d'être périmée, à savoir :

"SSE 25 - Le permis pour ENC <nom de la cellule> est arrivé à expiration. Cette cellule peut être périmée et NE DOIT PAS être utilisée pour la NAVIGATION primaire".

10.8.2 Données SENC périmées

Le client utilisateur de données doit vérifier l'état de la cellule ENC qui est affichée par rapport à l'état de cette cellule tel qu'il est connu au sein d'un service de fournisseur de données particulier. Ceci doit être effectué en comparant l'Edition actuelle [EDTN] et la mise à jour [UPDN] contenue dans le SENC pour toute cellule donnée par rapport à l'enregistrement de cellule correspondant dans le dernier fichier PRODUCTS.TXT.

Un avertissement permanent doit être émis lorsque la cellule ENC qui est affichée par l'ECDIS n'est pas mise à jour en fonction de la dernière nouvelle édition ou mise à jour en service, à savoir :

"SSE 27 –L'ENC<nom de la cellule > n'est pas mise à jour. Une nouvelle édition, une réédition ou une mise à jour de cette cellule manque et en conséquence elle NE DOIT PAS être utilisée pour la NAVIGATION primaire".

10.9 Procédures relatives à l'assurance qualité – Client utilisateur de données

10.9.1 Acceptation et vérification du certificat numérique de SA (et clé publique)

Un client utilisateur de données recevra la clé publique de SA sous deux formats, en tant que certificat numérique X.509 et en tant que clé publique imprimable. Le client utilisateur de données pourra charger le certificat numérique de SA et comparer manuellement la clé publique avec la clé publique imprimée (voir section 10.6.1.1). Le client utilisateur de données devra accepter la clé publique de SA, seulement lorsque cela aura été fait. Ce processus s'applique à la clé publique originale de SA ainsi qu'aux clés publiques subséquentes émises par le SA.

10.9.2 Création du permis d'utilisateur

Les fournisseurs d'application/système doivent pouvoir créer leur propre permis d'utilisateur qui contient le HW_ID chiffré. Le permis d'utilisateur sera fourni aux fournisseurs de données qui ensuite créeront les permis de cellule relatifs aux informations ENC demandées. Un permis d'utilisateur sera créé seulement pour demander des permis de cellule à un fournisseur de données.

10.9.3 Vérification du certificat de fournisseur de données

L'application du fabricant doit permettre la vérification du certificat de fournisseur de données contenu dans un fichier de signature ENC utilisant la clé publique du SA. Si le certificat du fournisseur de données passe la vérification avec succès, l'application extraira la clé publique du fournisseur de données à partir du certificat de fournisseur de données et l'utilisera pour vérifier la signature ENC.

Le SA précisera au fabricant les certificats de fournisseur de données qui n'ont pas été vérifiés avec succès.

10.9.4 Validation des permis de cellule

Le système du client utilisateur de données doit pouvoir valider l'intégrité d'un permis de cellule en contrôlant la somme de contrôle chiffrée. Ceci devra être fait en suivant la procédure mentionnée dans la section 10.5.4 de la Spécification.

Le client utilisateur de données doit pouvoir gérer les permis de cellule fournis par les fournisseurs de données. Le client utilisateur de données doit également pouvoir gérer les permis de cellule relatifs à une ENC fournie par des fournisseurs de données multiples.

Le client utilisateur de données doit pouvoir gérer les permis de cellule mémorisés de façon que les anciens puissent être supprimés et les nouveaux ajoutés, ou fusionnés, avec ceux qui sont stockés.

L'application du client utilisateur de données ne doit pas lui permettre de voir ni de copier les clés de cellule déchiffrées.

10.9.5 Authentification et déchiffrement des informations ENC

Le client utilisateur de données doit pouvoir accepter un ensemble de données signé et chiffré suivant la procédure définie dans les sections 10.6 et 10.7.

10.10 Procédures relatives à l'assurance qualité – Fabricants (OEM)

10.10.1 Contrat de confidentialité

Le SA donnera au fabricant des copies de toutes les informations nécessaires pour exploiter le dispositif de protection des données dans le cadre du contrat de confidentialité. Le fabricant devra respecter les conditions du contrat de confidentialité et faire en sorte que toutes les informations fournies soient actualisées.

10.10.2 Essai de conformité du système

Le fabricant réalisera les essais de conformité internes de la mise en application du dispositif de protection, basés sur les descriptions fournies dans ce document et sur les données d'essai.

Le SA n'émettra les M_ID et M_KEY qu'après le succès des essais de conformité attesté par le document d'auto-certification.

10.10.3 Stockage des M_ID et des M_KEY

Lorsque le fabricant adhèrera au dispositif, le SA fournira les informations spécifiques concernant les M_ID et les M_KEY pour créer les permis d'utilisateur.

Les utilisateurs de l'application du fabricant ne doivent pas pouvoir visionner ou extraire les informations relatives à M_KEY.

10.10.4 Création des HW_ID

Le fabricant pourra créer les HW_ID au format requis par la norme. Ils doivent être aléatoires et non séquentiels afin qu'ils ne puissent pas être reproduits.

Les utilisateurs de l'application du fabricant ne doivent pas pouvoir visionner ni extraire de l'application l'information HW_ID.

10.10.5 Enregistrement des HW_ID

Le fabricant doit enregistrer, dans un Registre HW_ID, les valeurs de chaque HW_ID créée. Ces détails doivent être mis à la disposition du SA sur demande.

Page laissée en blanc intentionnellement

11. Codes d'erreur de la S-63 et explications

Les codes d'erreur et les messages suivants sont définis dans les diagrammes des sections 0, 9, et 10. Il est prévu que les développeurs d'application indiquent les conditions d'erreur par un message d'erreur approprié. Lorsqu'une erreur se produit, ceci pourra empêcher dans certains cas le traitement ultérieur des données.

Code d'erreur	Message d'avertissement/d'erreur
SSE 01	*"Clé auto-signée invalide"*
SSE 02	*"Format de fichier de clé auto-signée incorrect"*
SSE 03	*"Certificat de SA signé du fournisseur de données invalide"*
SSE 04	*"Format de certificat signé du fournisseur de données incorrect"*
SSE 05	*"Fichier de certificat numérique de SA (X509) non disponible. Un certificat valide peut être obtenu à partir du site web de l'OHI ou de votre fournisseur de données".*
SSE 06	*"Le certificat de SA signé par le fournisseur de données est invalide. Le SA peut émettre une nouvelle clé publique ou l'ENC peut provenir d'un autre service. Une nouvelle clé publique de SA peut être obtenue à partir du site web de l'OHI ou de votre fournisseur de données.*
SSE 07	*"Le fichier de certificat de SA signé par le fournisseur de données n'est pas disponible. Un certificat valide peut être obtenu à partir du site web de l'OHI ou de votre fournisseur de données."*
SSE 08	*« Le format du fichier de certificat numérique de SA est incorrect. Un certificat valide peut être obtenu à partir du site web de l'OHI ou de votre fournisseur de données ».*
SSE 09	*"La signature ENC est invalide".*
SSE 10	*"Permis non disponibles pour ce fournisseur de données. Contacter votre fournisseur de données pour obtenir les permis corrects".*
SSE 11	*"Fichier de permis de cellule introuvable. Charger le fichier de permis fourni par le fournisseur de données".*
SSE 12	*"Format de permis de cellule incorrect. Contacter votre fournisseur de données et obtenir un nouveau fichier de permis.*
SSE 13	*"Format de permis de cellule invalide (somme de contrôle incorrecte). Contacter votre fournisseur de données et obtenir un nouveau fichier de permis".*
SSE 14	*"Date du système incorrecte; vérifier que l'horloge de l'ordinateur (si elle est accessible) est correctement installée ou contacter votre fournisseur de système".*
SSE 15	*"Service d'abonnement arrivé à expiration. Veuillez contacter votre fournisseur de données pour renouveler la licence d'abonnement.*
SSE 16	*"Valeur du CRC de l'ENC incorrecte. Veuillez contacter votre fournisseur de données car des données ENC peuvent être corrompues ou manquantes.*
SSE 17	*Permis d'utilisateur invalide (la somme de contrôle est incorrecte). Vérifier que le système mécanique (dongle) est connecté ou contacter votre fournisseur de données pour obtenir un permis d'utilisateur valide.*
SSE 18	*Format HW_ID incorrect*
SSE 19	*Permis non valides pour ce système. Veuillez contacter votre fournisseur de données pour obtenir les permis corrects.*
SSE 20	*Le service d'abonnement expirera dans moins de 30 jours. Veuillez contacter votre fournisseur de données pour renouveler la licence d'abonnement.*
SSE 21	*Le déchiffrement a échoué. Aucun permis de cellule valide trouvé. Les permis peuvent être valides pour un autre système ou de nouveaux permis peuvent être requis, veuillez contacter votre fournisseur de données pour obtenir une nouvelle licence.*
SSE 22	*Certificat numérique (X509) arrivé à expiration Une nouvelle clé publique de SA peut être obtenue à partir du site web de l'OHI ou auprès de votre fournisseur de données.*
SSE 23	*Mise à jour non séquentielle, précédentes mises à jour manquantes. Essayer de recharger à partir de supports de base. Si le problème persiste, veuiller contacter votre fournisseur de données.*

Code d'erreur	Message d'avertissement/d'erreur
SSE 24	*Format de signature ENC incorrect, veuillez contacter votre fournisseur de données.*
SSE 25	*Affichage – "Le permis pour l'ENC <nom de la cellule> a expiré. Cette cellule peut être périmée et NE DOIT PAS être utilisée pour la NAVIGATION primaire".*
SSE 26	*Cette ENC n'est pas authentifiée par l'OHI agissant en tant qu'Administrateur du dispositif*
SSE 27	*Affichage – "L'ENC<nom de la cellule > n'est pas à jour. Une nouvelle édition, une ré-édition ou une mise à jour pour cette cellule est manquante et donc ne DOIT PAS être utilisée pour la NAVIGATION primaire".*

SSE 01 doit être retourné lorsqu'une clé auto-signée (SSK) ne peut pas être validée par rapport à la clé publique stockée en tant que partie de la SSK. Le fournisseur de données doit vérifier que sa propre SSK est valide avant de renvoyer le certificat de SA signé par le fournisseur de données.

SSE 02 doit être retourné si la SSK est mal formatée. C'est-à-dire si des éléments ou des caractères de la SSK sont manquants. Le SA et les fournisseurs de données doivent compléter cette vérification.

SSE 03 doit être retourné si le certificat de SA signé par le fournisseur de données n'est pas authentifié correctement par rapport à la clé publique de SA. Ce processus de validation doit être réalisé par le SA avant qu'il ne soit remis au fournisseur de données. Le fournisseur de données doit valider le certificat de SA reçu du SA et le client utilisateur de données doit valider le certificat de SA contenu dans le fichier de signature ENC avant le déchiffrement.

SSE 04 doit être retourné si le certificat de SA signé par le fournisseur de données est mal formaté. Ceci doit être fait par le fournisseur de données à réception du certificat en provenance du SA.

SSE 05 doit être retourné s'il n'y a aucun certificat installé sur le système du client utilisateur de donnée ou si la voie d'accès ne peut être trouvée.

SSE 06 doit être retourné si le certificat de SA numérique (clé publique) n'est pas validé dans les cas suivants :

Le certificat numérique de SA n'est pas validée par rapport à la clé publique de SA.
La clé publique de SA contenue dans le certificat numérique n'est pas authentifiée par rapport à la signature contenue dans le fichier de signature ENC. Ce pourrait être le cas de certificat invalide ou de signature mal formatée ou invalide.

SSE 07 doit être retourné si le certificat de SA signé par le fournisseur de données n'est pas disponible pour le fournisseur de données ou n'est pas présent dans le fichier de signature ENC lorsque le client utilisateur de données tente de l'authentifier.

SSE 08 doit être retourné si la clé publique de SA contenue dans le certificat de SA numérique est mal formatée ou si le fichier de certificat n'est pas lisible.

SSE 09 doit être retourné si l'élément de la signature ENC dans le fichier de signature ENC n'est pas authentifié par rapport à la clé publique de fournisseur de données contenue dans l'élément de certificat du fichier de signature ENC.

SSE 10 doit être retourné s'il n'y a pas de permis de cellule disponible pour un fournisseur de données particulier correspondant à l'ensemble de données d'échange entrain d'être chargées.

SSE 11 doit être retourné s'il n'y a pas de permis installé sur le système.

SSE 12 doit être retourné si les permis de cellule sont formatés incorrectement.

SSE 13 doit être retourné si le CRC calculé du permis de cellule n'est pas validé par rapport au CRC détenu dans ce permis de cellule. [Clients utilisateurs de données]

SSE 14 doit être retourné si la date du système ne coïncide pas avec la date obtenue en provenance de toute source alternative, fiable, par exemple GPS. [Clients utilisateurs de données].

SSE 15 doit être retourné si la date d'expiration du permis de cellule est antérieure à celle obtenue à partir de la date de validation du système. [Clients utilisateurs de données].

SSE 16 doit être retourné si la valeur CRC calculée de l'ENC (après déchiffrement et décompression) n'est pas validée par rapport à la valeur CRC correspondante dans le CATALOG.031 file. Ceci s'applique également aux fichiers de signature, de texte et d'image déchiffrés. [Clients utilisateurs de données].

SSE 17 doit être retourné si le CRC contenu dans le permis d'utilisateur n'est pas validé par rapport au CRC calculé du HW_ID extrait. [Fournisseurs de données]

SSE 18 doit être retourné si le HW_ID déchiffré extrait du permis d'utilisateur est incorrectement formaté. [Fournisseurs de données]

SSE 19 doit être retourné si le HW_ID stocké à l'intérieur du système de sécurité mécanique/logiciel ne peut pas déchiffrer les permis de cellule entrain d'être chargés ou déjà installés dans le système.

SSE 20 doit être retourné si la licence d'abonnement doit arriver à expiration dans les 30 jours ou moins.

SSE 21 doit être retourné si une clé de cellule valide (clé de déchiffrement) ne peut pas être obtenue à partir du permis de cellule approprié pour permettre que le système déchiffre la cellule ENC correspondante.

SSE 22 doit être retourné si le certificat de SA numérique (X509) est arrivé à expiration. C'est-à-dire si la date dans la mention "Valide jusqu'au" est antérieure à la date validée sur le système.

SSE 23 doit être retourné si la mise à jour ENC importée n'est pas séquentielle à la dernière mise à jour déjà contenue dans le SENC pour toute cellule donnée. Dans ces conditions, le processus de mise à jour (pour la cellule) doit être terminé et l'ECDIS doit afficher un avertissement lorsque la cellule est affichée indiquant que la cellule n'est pas à jour et ne doit pas être utilisée pour la navigation.

SSE 24 doit être retourné si le format de signature ENC (première paire R & S) n'est pas compatible avec le format indiqué dans ce document. Dans ces conditions, le processus d'importation pour la cellule devrait être achevé mais le système devrait continuer à authentifier l'intégrité de toutes les cellules restantes.

SSE 25 doit être retourné si le permis ENC stocké pour chaque cellule donnée est arrivé à expiration Il devrait être possible de visualiser la cellule mais un message d'avertissement permanent devrait être affiché informant les utilisateurs, à savoir : "Le permis pour l'ENC <nom de cellule> est arrivé à expiration. Cette cellule est peut être périmée et NE DOIT PAS être utilisée pour la NAVIGATION primaire".

SSE 26 doit être retourné si le certificat de SA signé par le fournisseur de données est authentifié par rapport à un certificat ou à un fichier de clé publique stocké dans le système du client utilisateur de données, autre que celui fourni par le SA. Ceci convient dans les cas où plus d'un certificat ou d'une clé publique est stocké dans le système du client utilisateur de données.

SSE 27 doit être retourné si l'état de la cellule affichée n'est pas à jour par rapport au dernier fichier PRODUCTS.TXT chargé ou conservé dans le système. Un message d'avertissement permanent doit être affiché à l'écran pour informer l'utilisateur, par exemple « L'ENC < nom de cellule > n'est pas à jour. Une nouvelle édition, une nouvelle publication ou une mise à jour manque pour cette cellule et en conséquence elle NE DOIT PAS être utilisée pour la NAVIGATION primaire ».

Page laissée en blanc intentionnellement

S-63 Annexe A
Procédure de demande de certificat de fournisseur de données

Page laissée en blanc intentionnellement

1. Objectif

Le but de cette procédure est de définir le processus par lequel le fournisseur de données obtient du SA un certificat de fournisseur de données signé par le SA, tel que défini par la Norme de l'OHI S-63 Dispositif de protection des données.

2. Responsabilité

2.1 Besoin d'un certificat de fournisseur de données

Une organisation qui chiffre et signe numériquement les données ENC, en tant que partie intégrante de la S-63 Dispositif de protection des données de l'OHI, aura besoin d'un certificat de fournisseur de données signé par l'Administrateur du dispositif (SA).

Les utilisateurs de données ENC chiffrées ou signées numériquement (par exemple les systèmes ECDIS pour authentifier une signature et déchiffrer les informations ENC) n'auront pas besoin de certificat de fournisseur de données. Les agents ou les distributeurs qui fourniront uniquement des services ENC provenant d'un fournisseur de données n'auront pas besoin d'un certificat de fournisseur de données.

2.2 Services hydrographiques et organisations RENC

Tous les Services hydrographiques et les organisations RENC (Centre régional de coordination des ENC) auront seulement à compléter la partie I du formulaire ci-après et inclure les informations demandées pour solliciter un certificat de fournisseur de données. Un fournisseur de données peut obtenir un seul certificat de fournisseur de données.

2.3 Services non-hydrographiques et organisations non-RENC

Les autres organisations commerciales qui souhaitent agir en tant que fournisseurs de données, et qui chiffrent et signent numériquement les informations ENC conformes au dispositif de protection, peuvent solliciter un certificat de fournisseur de données. De telles organisations doivent obtenir qu'un fournisseur de données déjà membre du dispositif de protection, appuie la demande et complète la partie II du formulaire. Il est entendu que le fournisseur de données qui fournit les données ENC à l'organisation commerciale appuiera la requête.

2.4 Bureau hydrographique international

Le BHI en tant qu'administrateur du dispositif a la responsabilité exclusive de produire des certificats de fournisseur de données conformes aux procédures internes.

3. Definitions

Fournisseur de données: Il s'agit du terme utilisé pour désigner une organisation qui produit des données ENC chiffrées qui sont signées numériquement et émet des permis de cellule aux clients utilisateurs de données (utilisateurs finals).

Certificat: Les certificats sont des documents numériques attestant le lien entre une clé publique et un individu ou une organisation. Ils permettent de vérifier qu'une clé publique particulière appartient à une organisation spécifique, l'OHI dans ce cas.

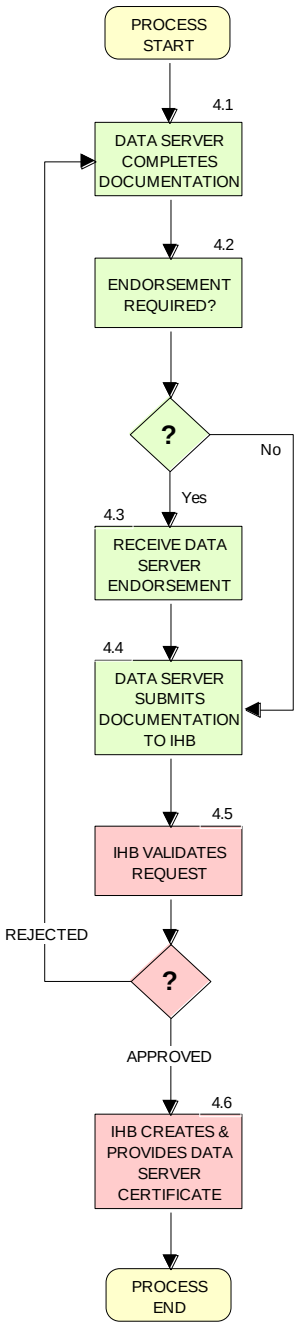
3.1 Références

[1] S-63 Dispositif de protection des données, Organisation hydrographique internationale

[2] S-57 Norme de transfert pour les données hydrographiques numériques, Organisation hydrographique internationale

4. Procédure

Ce chapitre définit la circulation des informations, les responsabilités et les instructions de travail.



4.1 Renseignement des formulaires et pièces jointes

- Un fournisseur de données, qui est déjà un Service hydrographique ou un RENC reconnu, et qui souhaite participer au dispositif de protection des données de l'OHI (S-63), doit fournir les informations suivantes au BHI :
- un contrat signé de fournisseur de données de l'OHI
- un formulaire de demande de certificat signé dont la partie I doit être renseignée
- la clé publique de fournisseur de données
- le certificat autosigné de fournisseur de données (SSK)

4.2 Autorisation nécessaire

Tous les services non hydrographiques et les organisations non RENC qui souhaitent devenir fournisseur de données doivent posséder un formulaire de demande de certificat appuyé par un fournisseur de données existant qui soit déjà membre du dispositif.

4.3 Organisation dont dépend l'autorisation

Le fournisseur de données qui appuie le formulaire de demande de certificat doit remplir la Partie II de celui-ci et le retourner aux services non hydrographiques ou à l'organisation non-RENC.

4.4 Soumission du formulaire de demande au BHI

Le fournisseur de données est responsable de la remise du formulaire de demande complétée ainsi que de toutes les autres informations listées dans la section 4.1 ci-dessus au BHI.

4.5 Validation de la demande de certificat

Le BHI validera les origines de la demande de certificat et authentifiera la clé publique en contactant le fournisseur de données. Il certifiera aussi que le besoin de certificat de fournisseur de données est applicable en contactant le fournisseur de données garante. Le BHI rendra compte des incohérences à l'initiateur de la demande.

4.6 Création du certificat de fournisseur de données

Le BHI est responsable de l'authentification de la SSK créée par le fournisseur de données. Si celle-ci est authentique le BHI signe alors la clé publique de fournisseur de données pour créer le certificat de fournisseur de données, celui-ci étant ensuite remis au fournisseur de données.

5. Evaluation de la qualité

Le BHI archivera les informations et les annexes de la demande du fournisseur de données, conformément aux procédures internes.

IHO S-63 Data Protection Scheme
Data Server Certificate Request Form

Ed.1-2003

Form to be returned to:
International Hydrographic Bureau
4, Quai Antoine 1er, B.P 445 - MC 98011 MONACO Cedex
Principality of Monaco
Tel: +(377) 93 10 81 00, Telefax: +(377) 93 10 81 40

Part I: To be completed by Data Server organisation

Organisation: .....
Address: .....
Address: .....
Address: .....
Postal number/place: ..... Country: .....
Tel: ..... Fax: ..... Web: .....

Administrative point of contact:	***Technical point of contact:***
Name:	**Name: .....**
Tel:	**Tel: .....**
E-mail:	**E-mail: .....**

Please verify the following information is included:
☐ All fields in Part 1 & 2 of this form are completed
☐ Data Server Public Key
☐ Data Server Self Signed Key (SSK)
☐ Signed IHO S-63 Data Server Agreement, or ☐ already available with IHB

Signed date: ..... Name: .....

Part II: To be completed by endorsing HO or RENC organisation

Organisation: .....
Contact name: .....
Tel: ..... Fax: ..... E-mail: .....

Part III: To be completed by IHB

☐ Form and attachments validated
☐ Signed Data Server Agreement, ref. ……
☐ Certificate created date: ..... File ref: .....
☐ Certificate returned to Data Server

Signed date: ..... Name: .....

Page laissée en blanc intentionnellement

Annexe B à la S-63
Procédure de demande d'information du fabricant

Page laissée en blanc intentionnellement

1. Objectif

Le but de cette procédure est de définir le processus que le fabricant doit suivre dans le but de faire partie du dispositif de protection des données de l'OHI (Norme S-63). Pour ce faire, les fabricants exigeront leurs propres valeurs M_ID et M_Key spécifiques. Celles-ci seront fournies par le SA, telles que définies dans la Norme de l'OHI S-63 Dispositif de protection des données, de sorte que le fabricant puisse déchiffrer les ENC chiffrées avec la norme S-63.

2. Responsabilité

2.1 Fabricants (OEM)

Seuls les fabricants qui développent les applications du client utilisateur de données ont besoin de valeur unique de M_ID et M_KEY. Le BHI, en tant qu'administrateur du dispositive, partagera cette information avec tous les fournisseurs de données participant au dispositif. Une seule combinaison M_ID et M_KEY sera forunie au fabricant.

Les valeurs M_ID et M_KEY seront restituées au SA si l'organisation cesse les échanges commerciaux ou si elle ne supporte pas une application pour accéder et afficher les ENC chiffrées avec la norme S-63. Les fournisseurs de données seront informés de tels cas de sorte qu'aucune nouvelle licence ne sera émise pour ce système particulier de fabricant.

Le client utilisateur de données n'aura pas besoin d'avoir accès à la valeur M_KEY parce qu'elle est incorporée de façon sécurisée dans l'application de l'utilisateur final (c'est-à-dire dongle) et fournie aux clients utilisateurs de données sous une forme chiffrée appelée permis d'utilisateur.

2.2 Bureau hydrographique nternational

Le BHI en tant que SA a la responsabilité exclusive de produire les valeurs M_ID et M_KEY, de les fournir aux fabricants et de les distribuer aux fournisseurs de données.

3. Définitions

M_ID: Identification du fabricant
M_KEY: Clé du fabricant
OEM: Fabricant de l'équipement d'origine
Permis d'utilisateur: Une chaîne de 28 caractères alphanumériques contenant le HW_ID chiffré du client utilisateur de données ainsi que la M_KEY et contenant la M_ID.
Dongle: Un système mécanique codé qui contient le HW_ID du système du client utilisateur de données.

3.1 Références

[1] S-63 Dispositif de protection des données, Organisation hydrographique internationale
[2] S-57 Norme de transfert pour les données hydrographiques numériques, Organisation hydrographique internationale

4. Procédure

Ce chapitre définit la circulation des informations, les responsabilités et les instructions de travail détaillées.

4.1 Renseignement du formulaire de demande

Le fabricant est chargé de fournir tous les renseignements de la partie I du formulaire de demande M_ID et M_KEY ci-joint. L'OHI peut demander plus ample documentation telle que des contrats de confidentialité – ces derniers ne sont pas indiqués ici.
On note qu'un fabricant :

- Ne peut recevoir qu'une seule paire de M_ID et M_KEY.
- Doit restituer les informations au SA si ce dernier arrête les échanges commerciaux ou ne livre pas les produits authentifiant les signatures ou n'a plus besoin de déchiffrer les informations ENC.

4.2 Vérification du formulaire de demande

Le SA vérifie que tous les renseignements dans la partie 1 du formulaire sont fournis, ou donne au fabricant les informations concernant les renseignements manquants.

4.3 Vérification du contrat de confidentialité signé

Le SA vérifie qu'un contrat de confidentialité signé est inclus avec la demande ou est déjà disponible dans les archives du BHI. Si un contrat n'est pas disponible, le SA informe le fabricant de l'obligation d'un contrat signé.

4.4 Vérification du succès des essais grâce aux données d'essais S-63

Le SA vérifie que le fabricant a conclu avec succès les essais de l'application avec les données d'essai de la norme de l'OHI S-63. Dans le cas contraire, il est demandé au fabricant de terminer la procédure d'essais définie avant de fournir M_ID et M_KEY.

4.5 Vérification que l'OEM n'est pas déjà en possession de M_ID et M_KEY

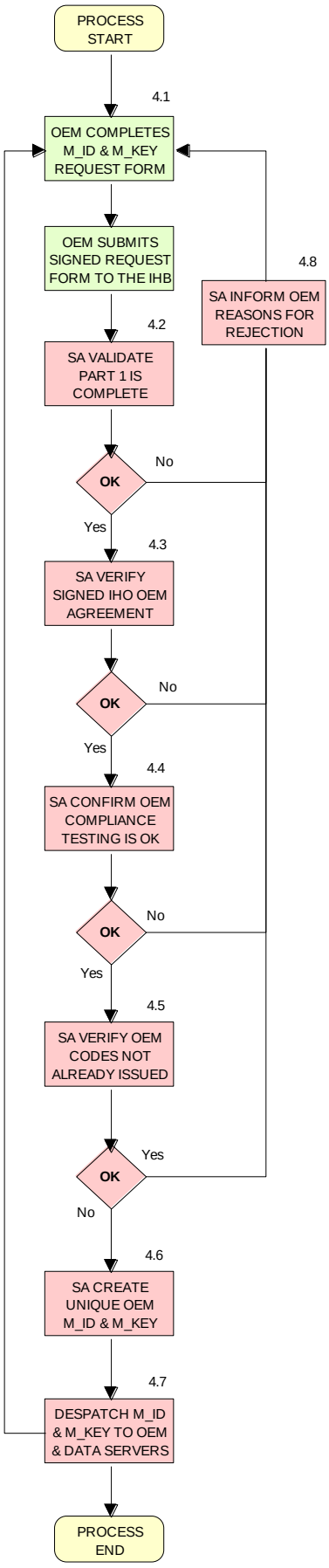
Le SA vérifie que M_ID et M_KEY n'ont pas déjà été attribués au fabricant. Dans le cas contraire, le SA signale le problème au fabricant.

4.6 Création de M_ID et M_KEY

Le SA attribue au fabricant une combinaison disponible et unique de M_ID et M_KEY.

4.7 Informer l'OEM sur les nouvelles M_ID et M_KEY

Le SA donne au fabricant des informations sur ses M_ID et M_KEY. Le SA donne des informations à tous les fournisseurs de données enregistrés sur les nouvelles M_ID et M_KEY.



4.8 Informer l’OEM sur les problèmes concernant la demande

Le SA informe le fabricant sur les problèmes spécifiques concernant la demande et demande que des informations à jour soient fournies avant l’attribution de M_ID et de M_KEY. Le traitement de la demande est terminé.

5. Evaluation de la qualité

Le BHI archivera le formulaire de demande et toutes les informations relatives, conformément aux procédures internes.

IHO S-63 Data Protection Scheme
M_ID and M_KEY Request Form

Ed.1-2003

Form to be returned to:
International Hydrographic Bureau
4, Quai Antoine 1er, B.P 445 - MC 98011 MONACO Cedex
Principality of Monaco
Tel: +(377) 93 10 81 00, Telefax: +(377) 93 10 81 40

Part I: To be completed by OEM organisation

Organisation: .....
Address: .....
Address: .....
Address: .....
Postal number/place: ..... **Country:** .....
Tel: ..... **Fax:** ..... **Web:** .....

Administrative point of contact:	***Technical point of contact:***
Name:	**Name:** .....
Tel:	**Tel:** .....
E-mail:	**E-mail:** .....

***Please verify the following information is included*:**

☐ All fields in Part 1 of this form are completed
☐ Signed IHO S-63 OEM Agreement, or ☐ already available with IHB
☐ Completed successful testing of application with the M_ID and M_KEY provided with the S-63 test dataset

Signed date: ..... Name: .....

Part II: To be completed by IHB

☐ Verify Part 1 is completed
☐ Signed OEM Agreement available, ref. .....
☐ Verify OEM does not have a previously issued M_ID and M_KEY
☐ Assigned M_ID: ..... M_KEY: .....
☐ M_ID and M_KEY returned to OEM and all registered Data Servers

Signed date: ..... Name: .....

S-63 Appendice 1
Données d’essai du dispositif de protection des données

Page laissée en blanc intentionnellement

Note importante: L'appendice 1 de la S-63 comprend les données d'essai qui sont fournies séparément sous forme de fichiers compressés (ZIP) (voir la section S-63 sur le site web de l'OHI). Intégré dans le fichier ZIP, se trouve un document "Guide de mise en application des données d'essais" qui fournit des instructions sur l'utilisation des données d'essai. Le texte ci-dessous donne une brève présentation de l'appendice 1.

1. Introduction

L'appendice 1 de la S-63 définit un ensemble de définitions d'essai et de données d'essai recommandé qui peut être utilisé par les développeurs d'applications de fournisseur de données et de client utilisateur de données pour comprendre les structures de sécurité définies dans la S-63 et tester si leurs applications sont conformes à la Norme. Elle inclut un Guide de mise en application des données d'essai [Test Data Implementation Guide] qui est fourni avec les données d'essai.

L'appendice 1 de la S-63 sera mise à jour par le Groupe de travail sur la structure de protection des données (DPSWG de l'OHI). Dans le futur, un plus grand nombre de données d'essai pourront être incluses, selon les retours d'information de l'utilisateur, pour fournir une plate-forme complète d'essai destinée à vérifier l'exactitude et la conformité avec la norme, ou en ce qui concerne les applications de l'utilisateur final, pour identifier les cas d'erreur. La version actuelle du document fournit un exemple d'essai complet pour les tests de conformité..

Le Guide de mise en application des données d'essai ("Test Data Implementation Guide") auxiliaire sera mis à jour indépendamment du document principal de la S-63 de l'OHI et de nouvelles versions seront publiées sur le site web de l'OHI.

2. Organisation des définitions d'essai et des données d'essai

2.1 Définitions d'essai

Les définitions d'essai offrent des essais fonctionnels de haut niveau qui sont recommandés pour tester la conformité des structures de sécurité définies dans la S-63. Elles ne remplacent pas le test unitaire dans le développement du logiciel, mais offrent des entrées structurées pour les essais de logiciel functionnel.

Les définitions d'essai sont agencées par catégories fonctionnelles et définies au chapitre 3 du Guide de mise en application des données d'essai » ("Test Data Implementation Guide"). Les définitions d'essai pour les fonctionnalités du SA n'ont pas été incluses dans le document puisque seul le BHI aura besoin de ces scénarios d'essai.

Chaque définition d'essai indique si le test est applicable aux applications du fournisseur de données ou du client utilisateur de données. Il est à noter qu'un essai est valable pour toute application si le type d'application n'est pas indiqué.

Il y a des définitions d'essai à la fois pour les conditions d'essai justes et erronées pour assurer une application robuste et refléter les conditions d'opération.

Il est à noter que la CEI sera chargée de définir les essais d'approbation applicables aux ECDIS, qui seront un complément à ce document.

2.2 Données d'essai

Une gamme de données d'essai a été développée pour appuyer les définitions d'essai. Les caractéristiques de chaque ensemble de données d'essai sont définies dans le chapitre 4 du Guide de mise en application des données d'essai ("Test Data Implementation Guide").

Toutes les données d'essai sont classées dans un fichier ZIP et seront extraites à l'intérieur d'une structure de répertoire où chaque donnée d'essai sera placée dans un répertoire séparé. Il est à noter que certains ensembles de données d'essai seront utilisés dans plusieurs définitions de tests.

Il est à noter également que les données d'essai peuvent être utilisées par les développeurs pour des tests unitaires ou d'autres types d'essai concernant leur application.

2.3 Conditions d'utilisation des données d'essai

Les informations ENC (le matériel) incluses dans les données d'essai ont été mises à disposition du destinataire dans le seul but de tester son application et de vérifier sa conformité avec la norme S-63. Le matériel est fourni selon les conditions décrites ci-dessous. Si le destinataire n'est pas d'accord pour remplir ces conditions, le matériel ne peut être utilisé et devra donc être détruit.

5.1.1 2.3.1 Conditions de fourniture des données

Le matériel fourni est protégé par le droit d'auteur du Service hydrographique national. Aucune partie du matériel fourni ne peut être reproduite, stockée dans un serveur ou transmise sous quelque forme ou quelque moyen que ce soit – électronique, mécanique ou de reproduction – excepté le matériel nécessaire pour remplir le but décrit ci-dessus.

Le matériel ne doit PAS être utilisé pour la navigation.

Lorsque le matériel n'est plus nécessaire pour remplir le but, il doit être détruit ainsi que les copies de travail.

5.1.2 2.3.2 Exonération de responsabilité

Bien que le BHI et les Services hydrographiques fassent tous les efforts possibles pour faire en sorte que le matériel soit bien adapté au but, ils n'offrent cependant pas de garantie ni d'autres assurances qu'il remplit bien les conditions requises. Le BHI et les Services hydrographiques n'accepteront aucune responsabilité pour quelque préjudice ou perte que ce soit venant de son utilisation. Le destinataire utilise le matériel fourni entièrement à ses propres risques.

S-63 Appendice 2
[Média de grande capacité]

.

Page laissée en blanc intentionnellement

1. Introduction

Jusqu'à récemment la majorité des ECDIS/ECS avaient seulement la capacité de charger des ensembles de données d'échange ENC (ExSets) à partir des CD-ROM. Toutefois, il est devenu de plus en plus courant que les systèmes de fabricants soient livrés avec des lecteurs DVD ou d'autres média de grande capacité[1] LMS). L'inclusion de ces supports de grande capacité offrent maintenant aux fournisseurs de données la possibilité d'inclure plus de données ENC sur un seul support.

Plusieurs questions sont apparues au cours de l'exploitation des services existants pour ENC chiffrées avec l'édition 1.0 de la norme S-63. Non des moindres est le fait que fournir de larges ensembles de données d'échange a eu pour conséquence un temps de chargement inacceptable pour les ECDIS/ECS. C'est une des raisons de principe pour lesquelles les fournisseurs de données ne fournissent pas de services qui incluent des ensembles de données d'échanges uniques s'étandant sur des CD-ROM multiples.

Stocker un seul ensemble de données d'échange pour ENC sur une mémoire de grande capacité, telle un DVD ou une clé USB, qui serait de la même taille qu'un ensemble stocké sur un CD-ROM représenterait une mauvaise utilisation inéfficace du support et de la mémoire disponible. Dans ce cas, il serait plus avisé de stocker des ensembles de données d'échange multiples sur le même support, chacun étant approximativement de la même taille que ceux stockés actuellement sur CD-ROM. Puisque cette méthode de stockage n'est pas définie dans les Spécifications de produit de la S-57 de l'OHI ou de l'Edition 1.0 de la S-63 une nouvelle configuration devra être spécifiée.

Au cours de l'élaboration de la structure du média les considérations suivantes devront être prises en compte:

- Les services ENC pourront être fournis sur des ensembles multiples de média
- Les services ENC pourront contenir des données provenant de plus d'un fournisseur de données
- Les fichiers appropriés devront être fournis de façon à ce que les systèmes de fabricants puissent gérer et importer les ENC chiffrées avec la norme S-63 d'une façon efficace et rapide et créer des systèmes intuitifs qui gérent facilement de multiples parties de média.

2. Vue d'ensemble des supports

La section suivante donne une vue d'ensemble de la manière dont les données seront structurées sur les supports. Elle souligne également comment la structure des ensembles de données d'échange de la S-63 a été modifiée pour les supports de grande capacité; ceci est encore renforcé par les diagrammes des annexes A et B de cette appendice. Des renseignements détaillés portant sur le contenu et le format de ces dossiers et de ces fichiers sont fournis plus avant dans cette appendice.

2.1 Types de supports

Il y aura deux types de supports, le support de "BASE", qui contient un ou plusieurs ensembles de données d'échange de base et le support de "MISE A JOUR ", qui contient les mises à jour hebdomadaires pour ENC, lesquelles peuvent se trouver dans un ou plusieurs ensembles de données sur le support de mise à jour. On estime que du fait de l'accroissement de capacité qu'offrent ces types de support, il serait possible de ré-éditer les ensembles de données d'échange de base sur le support de mise à jour et inversement les mises à jour hebdomadaires sur les supports de base.

---

[1] Support de grande capacité fait également référence aux mémoires de grande capacité**.**

2.2 Structure des supports de dossiers et fichiers

Tous les ensembles de données d'échange se trouvent dans le répertoire souche de chaque support, chacun dans son propre sous-répertoire. La configuration de tous les ensembles de données d'échange est la même que celle indiquée en 7.5.1 du document principal avec une seule exception notable. Le dossier « INFO » qui inclut le fichier "PRODUCTS.TXT" ne sera plus stocké dans le répertoire souche de l' (es) ensemble (s) de données mais dans le répertoire souche du support.

Le dossier "INFO" continuera d'être utilisé par les fournisseurs de données pour inclure les fichiers supplémentaires spécifiques à leurs services pour ENC chiffrées avec la norme S-63. Il faut noter que tout fichier spécifique de fournisseurs de données stocké dans ce dossier doit être nommé de façon à ce qu'il n'y ait pas de contradiction avec la convention de dénomination des fichiers de la S-63.

2.2.1 Fichier additionnel de support

Un fichier additionnel nommé "MEDIA.TXT" sera inclus sur chaque support pour aider les clients utilisateurs de données à gérer les ensembles de données d'échange multiples sur le même support et entre des ensembles de support multiples. Il permettra également aux systèmes des clients utilisateurs de données de pousser les utilisateurs à insérer le support approprié en incluant une chaîne lisible par la machine dans chaque enregistrement faisant référence à chacun des médias. Une explication plus détaillée du format de fichier MEDIA.TXT est fourni plus loin en section 3.

2.3 Identification du support

Il doit y avoir une méthode pour différencier les services fournis sur CD-ROM et ceux fournis sur support de grande capacité. Le premier différenciateur est l'ID du volume du support (voir section 2.3.1), qui identifiera l'utilisation du format de grande capacité et notifiera au client utilisateur de données la structure prévue du dossier et du fichier.

La présence du nouveau MEDIA.TXT en tant que répertoire souche du support est une indication supplémentaire que le service ENC est fourni en utilisant un support de grande capacité.

2.3.1 Labélisation du support

Pour ce qui concerne les supports de grande capacité, la convention de labélisation du support sera semblable à celle utilisée dans la spécification de produit de la S-57 de l'OHI. Au lieu de "V01X01", ou "V" représente le "Volume", la lettre "M" pour "Media" lui sera substituée.

Le label du volume concernant le support de grande capacité indiquera également combien d'ensembles de support sont en service. En conséquence, s'il y a trois ensembles de support, ils seront labélisés de la manière suivante:

M01X03 [Ensemble de support 1 sur 3]
M02X03 [Ensemble de support 2 sur 3]
M03X03 [Ensemble de support 3 sur 3]

NOTE: Ceci représente uniquement le nombre d'ensembles de support dans un service ENC et n'implique pas qu'il s'agisse d'un seul ensemble de données d'échange couvrant de multiples ensembles de supports.

3. Formats de support de fichier

3.1 Listing de produit (PRODUCTS.TXT)

En ce qui concerne le "Support de base", le fichier "PRODUCTS.TXT" contiendra les enregistrements relatifs à toutes les cellules contenues sur ce support particulier. L'en-tête tel que défini dans la section 6.2.2 du document principal sera étiquetté "COMPLET" s'il existe un seul support pour un service particulier. Cependant, s'il existe plus d'un support, il sera libellé "PARTIEL". Un listing de produits "COMPLET" sera toujours fourni sur le "Support de mise à jour » avec les enregistrements de toutes les cellules dans un service de fournisseurs de données.

Il est important que les fabricants d'ECDIS/ECS gèrent ces enregistrements avec soin; les listings de produits " PARTIELS " doivent être fusionnés avec le listing "COMPLET" stocké à l'intérieur du système. Il est à noter que le système peut contenir des informations relatives aux produits de plus d'un seul fournisseur de données. Toutefois, il est important de ne pas écraser les listings "COMPLETS" à moins qu'ils ne soient stockés indépendamment selon le fournisseur de données.

3.2 Listing des supports (MEDIA.TXT)

Il s'agit d'un nouveau fichier destiné à gérer les services fournis en utilisant le support de grand capacité. Il est situé dans le répertoire principal du support de base et de mises à jour et contient des informations relatives à l'ensemble des supports d'un service de fournisseur de données et aux ensembles de données d'échange contenu sur un support. Le but principal de ce fichier est le suivant :

Fournir aux clients utilisateurs de données un moyen de gérer les importations d'un service de fournisseur de données qui peut recevoir des supports à grande capacité.
Fournir des informations pour permettre aux clients utilisateurs de données de gérer des ensembles à supports multiples.
Fournir des renseignements exploitables par la machine de manière à ce que les clients utilisateurs de données puissent rendre le processus d'importation plus intuitif pour l'utilisateur final.

NOTE: Le support de mises à jour le plus récent contiendra toujours le dernier état des ensembles des données de base contenus dans un service de fournisseur de données. Ceci peut être utilisé afin de vérifier que l'ensemble de données d'échange de base le plus récent a été installé. De plus amples détails quant à la structure et au format de ce fichier sont donnés ci-dessous :

3.2.1 Format d'en-tête

L'objectif de l'en-tête du MEDIA.TXT est le même que celui du fichier SERIAL.ENC stocké dans avec l'ensemble de données d'échange. Il est utilisé pour gérer l'installation du support en identifiant les points suivants :

- Le fournisseur de service du support
- La date et la semaine d'émission du support
- Le numéro du support et le type de support
- Le nom du support exploitable par la machine devant être affiché pour les utilisateurs

L'en-tête est fourni sur deux lignes qui contiennent chacune un seul enregistrement; le premier à une longueur fixe, et le second est séparé par une virgule. Le tableau suivant définit le format plus en détail:

Champ ID	Domaine	Octets	Portée
ID du fournisseur de données	Caractère	2	Toute paire alphanumérique, par ex. PR
Semaine d'émission	Caractère	10	Tout caractère ASCII par exe. WKNN_YY
Date d'émission	Date	8	YYYYMMDD
Type de support	Caractère	10	BASE ou MISE A JOUR
Label d'identification du support	Caractère	6	M[01-99]X[01-99]
Fin du délimiteur d'enregistrement	hexadécimal	2	CR/LF
ID du support	Caractère	2-3	Par exemple, M1, M2 ou M11.
Nom du support exploitable en machine	'Caractère'	0-100	Chaîne de texte entre guillemets
Information régionale [Optionnel]	'Caractère'	0-100	Chaîne de texte entre guillemets
Fin du délimiteur d'enregistrement	hexadécimal	2	CR/LF

Exemple:

```
GBWK27_07   20070621BASE      M01X03
M1,'UKHO Week 27_07 BASE MEDIA 1','Europe, Africa, and Middle East'
```

3.2.2 Format d'enregistrement du support

Le fichier "MEDIA.TXT" contient également une liste d'enregistrement qui identifie tous les ensembles de données d'échange dans un service de fournisseur de données et le support de destination où ils peuvent être localisés. Son objectif est de fournir aux clients fournisseurs de données un moyen de gérer l'importation des ENC chiffrées à travers des ensembles à supports multiples et des renseignements exploitables en machine de façon à ce que le client utilisateur de données puisse inciter les utilisateurs finaux à utiliser le support approprié.

Le fichier "MEDIA.TXT" stocké sur le support de MISE A JOUR contiendra toujours une liste COMPLETE des ensembles de supports contenu dans le service de fournisseur de données. Il renfermera également la date à laquelle le support a été dernièrement utilisé, de cette manière les systèmes ECDIS/ECS peuvent toujours prouver qu'ils renferment les informations les plus récentes.

Le fichier "MEDIA.TXT" stocké sur le support de BASE contien une liste des ensembles de données d'échange stockés sur le support. Il ne contiendra pas d'information sur les autres volumes du service.

Champ ID	Domaine	Octets	Portée	Notes (voir ci-dessous)
Emplacement du support/ ensemble de données	Caractère	5-7	M1 to M99;B1 to B99 e.g. M2;B7 [Media 2, Base ExS 7] M1 to M99;U1 to U99 e.g. M1;U2 [Media 1, Update ExS 2]	1
Date d'émission de l'ensemble de données d'échange	Date	8	YYYYMMDD, e.g. 20070621	2
Numéro de support de l'ensemble de données [Nom long]	Caractère		'Tout caractère ASCII '	3
Information régionale [Optionnel]	Caractère		'Tout caractère ASCII '	4
Champ reservé	Caractère			5
Champ des commentaires	Caractère			6

Exemple:
```
M1;B1,20070614,'Base Dataset 1',Europe',,
```

Notes:

1. Ce champ identifie le support sur lequel l'ensemble de données d'échange (base ou mise à jour) est localisé.
2. Date d'émission de l'ensemble de données d'échange. Il s'agit de la date à laquelle un ensemble de données d'échange est émis ou ré-émis[2] sur le support (base ou mise à jour). Bien qu'il puisse être plus pratique d'émettre à nouveau des ensembles de données d'échange simultanément sur un support spécifique, il peut y avoir des cas où le support est ré-émis avec un seul ensemble de données d'échange ré-émis. Les clients utilisateurs de données peuvent utiliser cette date pour valider l'état des cellules actuellement installées à partir du support de mise à jour.
3. Il s'agit d'une chaîne de texte exploitable par la machine que les clients utilisateurs de données peuve utiliser pour inciter les utilisateurs finals à charger le support approprié.
4. Il s'agit d'une chaîne de texte exploitable en machine, optionnelle, qui peut être utilisée par les clients utilisateurs de données pour visualiser les informations additionnelles relatives aux régions/pays producteurs sur un support spécifique.
5. Utilisation future
6. Commentaires additionnels.

Le fichier de support de mise à jour ***"MEDIA.TXT"*** contiendra toujours les dates d'émission les plus récentes et les informations relatives aux ensembles de données d'échange du support de base dans un ensemble de support. *Bien que des dispositions aient été prises pour avoir plus qu'un ensemble de données d'échange à jour sur un support de mise à jour, ce n'est pas recommandé pour les raisons exposées à la section 7. Toutefois, s'il y en a plus d'un, ce peut être géré par les entrées dans les fichiers PRODUCTS.TXT et MEDIA.TXT sur le support de mise à jour.*

Exemple d'un fichier **MEDIA.TXT [MISE A JOUR]:**

```
GBWK28_07   20070628UPDATE    M01X02
U1,'UKHO Week 28_07 UPDATE MEDIA 1 of 2','Europe'
M1;B1,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M1;B2,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M1;B3,20070621,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M2;B4,20070517,'UKHO BASE MEDIA 2','North and South America',,
M2;B5,20070517,'UKHO BASE MEDIA 2','North and South America',,
M3;B6,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,
M3;B7,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,
```

Exemple d'un fichier **MEDIA.TXT [BASE] complet :**

```
GBWK27_07   20070621BASE      M01X03
M1,'UKHO Week 27_07 BASE MEDIA 1','Europe, Africa, and Middle East'
M1;B1,20070614,'Base Dataset 1',Europe',
M1;B2,20070614,'Base Dataset 2','Africa',,
M1;B3,20070621,'Base Dataset 3','Middle East',,
```

[2] Un ensemble de données d'échange réédité est un ensemble qui contient la base entière des ENC (plus les mises à jour) qui lui sont attribuées plus toutes nouvelles éditions et mises à jour produites depuis sa publication/réédition.

4. Gestion des supports (Fournisseurs de données)

L'émission et la ré-émission des supports de base dépendent en grande partie du fournisseur de données. Toutefois, pour éviter le renouvellement continu des supports de base, il est recommandé que les ensembles de données d'échange individuel ne soient pas émis indépendamment les uns des autres sur le même support. Toutefois, il peut y avoir des cas où cela s'avère nécessaire, par exemple lors de l'introduction des ENC d'un nouveau pays ou du nécessaire contrôle de l'ensemble des données d'échange de mise à jour.

Si un fournisseur de données exploite au deux tiers un service, par exemple s'il soutient à la fois les services sur CD-ROM et sur DVD. Le contenu des ensembles de données d'échange de base et de mise à jour sera identique dans les deux services. Il se pourrait que le fournisseur de données émette les ensembles de données d'échange de base sur DVD et les mises à jour officielles hebdomadaires sur CD-ROM. Ceci permettra de maintenir les coûts de production à leur minimum.

5. Gestion des supports (Clients utilisateurs de données)

Etant donné que le volume des ENC continue d'augmenter, une méthode plus intelligente et plus « habile » de les charger dans l'ECDIS/ECS est requise. Puisque la plupart des clients n'achète qu'un sous-élément de l'ensemble des ENC disponibles, il semblerait prudent de baser l'importation des ENC chiffrées selon la norme S-63 directement sur les clients détenant des permis. Les points suivants sont fournis à titre d'exemple des étapes recommandées pour l'importation des ENC chiffrées.

- Insérer, lire et valider le fichier **'PERMIT.TXT'**
- Insérer le **'Support de mise à jour'**
- Lire le listing de produits ***"COMPLET"*** qui forme le fichier **'PRODUCTS.TXT'**
- Identifier et marquer toutes les cellules qui possèdent une licence (qui ont des permis valides).
- Identifier la cible **'Support de base'** et **'Ensemble d'échange de données'** de chaque ENC autorisée.
- Pousser l'utilisateur à installer le **'Support de base'** approprié
- Installer toutes les ENC autorisées à partir des **'Support de base'** et **'Ensemble de données d'échange'**
- Pousser l'utilisateur à insérer le plus récent **'Support de mise à jour'** dans le but de mettre à jour toutes les ENC autorisées et à compléter le cycle de chargement des ENC.

NOTE: Dans le cas de données ENC chiffrées, il n'est pas nécessaire ou souhaitable de lire le fichier CATALOG.031 en entier. Ce fichier ne devra être utilisé que pour identifier la cible de toutes les ENC autorisées et de tout fichier associé dans l'ensemble de données d'échange.

5.1 Avertissements relatifs au support

Au moment du chargement du support de mise à jour hebdomadaire les clients utilisateurs de données doivent contrôler que la date d'émission des ensembles de données d'échange installés sont récents et à jour. Le dernier support de mise à jour contiendra toujours la dernière date d'émission de chaque ensemble de données d'échange à l'intérieur du service dans le fichier "MEDIA.TXT".

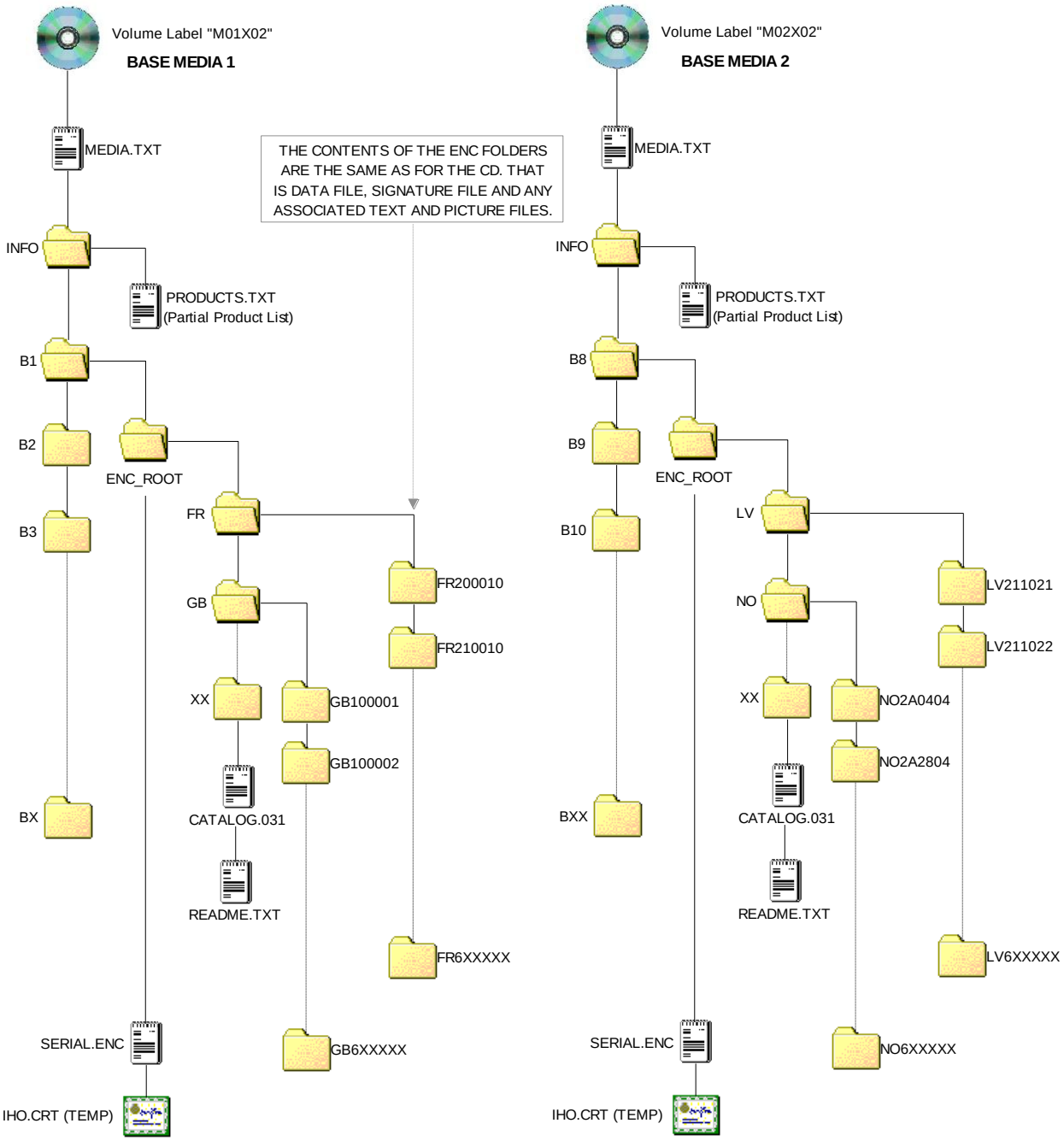
Si le dernier support de base n'est pas chargé dans l'ECDIS/ECS, un avertissement doit être donné à l'utilisateur pour l'informer, comme par exemple:

'Media X', 'Base Exchange Set Y' a été émis à nouveau, il peut être impossible d'installer des mises à jour. Merci de bien vouloir charger le dernier 'Media X' avec la date d'émission du 'YYYYMMDD'

ANNEXE A

BASE MEDIA FOLDER AND FILE STRUCTURE

The diagram below is for illustrative purposes only and outlines the top level folder and file structure that must be used by data servers when supplying S-63 encrypted ENC services utilising large media support. However, it is possible that the structure under each ENC_ROOT folder of each exchanges set may vary between data servers.

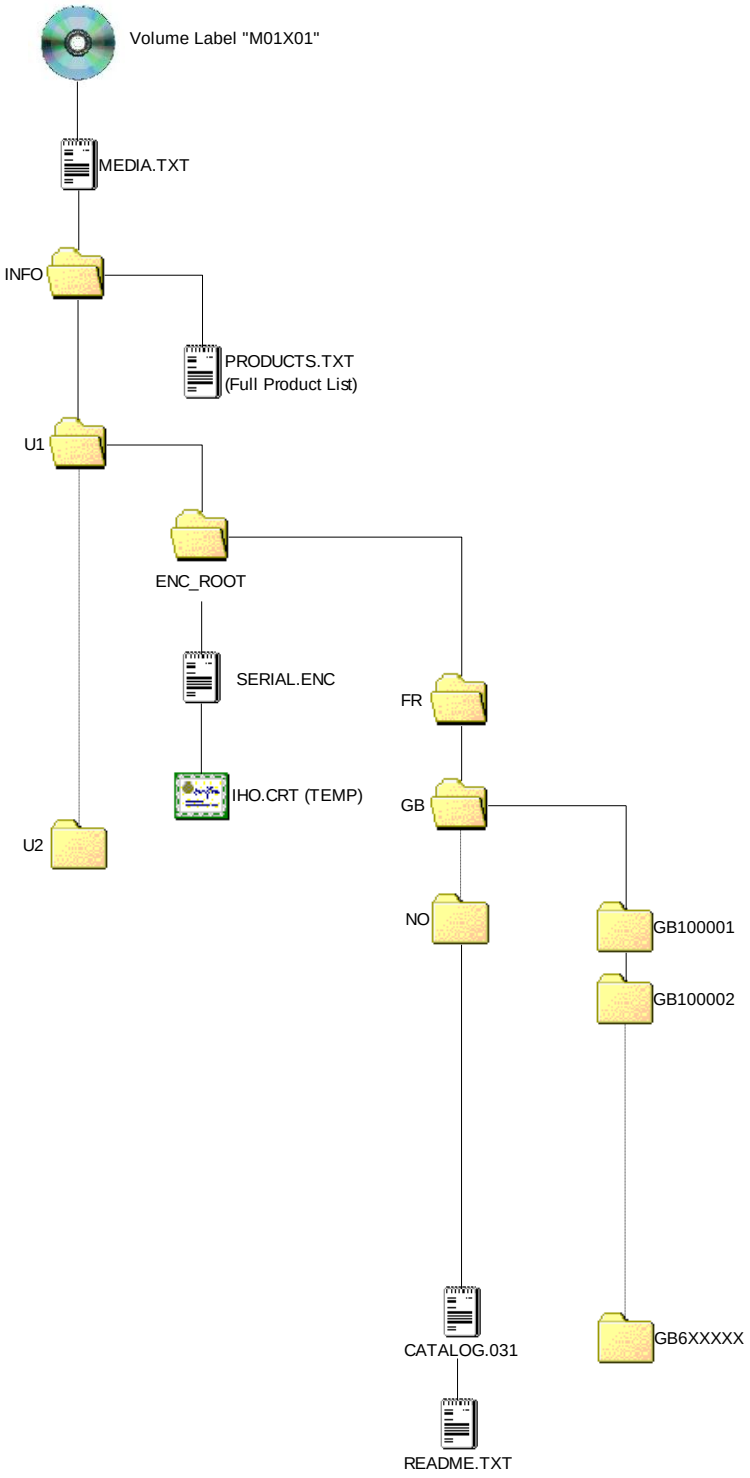


LARGE MEDIA SUPPORT FOR S-63 ENCRYPTED ENC SERVICES
BASE MEDIA FOLDER AND FILE STRUCTURE

ANNEXE B

UPDATE MEDIA FOLDER AND FILE STRUCTURE

The diagram below is for illustrative purposes only and outlines the top level folder and file structure that must be used by data servers when supplying S-63 encrypted ENC services utilising large media support. However, it is possible that the structure under each ENC_ROOT folder of each exchanges set may vary between data servers.



UPDATE MEDIA STRUCTURE
(Only top level folders & files)