

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

*Ministère de l'enseignement supérieur*

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE  
HOUARI BOUMEDIENE  
(USTHB)

INSTITUT D'INFORMATIQUE

*Mémoire de fin d'études*

*Développement d'un environnement  
sécurisé pour le système EDI*

*EDISTEC*

*Promotrice : M<sup>me</sup> A. EL-MAOUHAB*

*Co-promoteur : M. F. RAHAL*

*Réalisé par : M<sup>lle</sup> CHEBCHOUBI SOUAD*

*M<sup>lle</sup> ESSED NABILA*

*Centre d'accueil : Centre de Recherche sur l'Information  
Scientifique et Technique*

*Promotion 1998*

# Sommaire

## *1<sup>ère</sup> Partie : Concepts de base*

1. Introduction .....	1
2. Concept de l'EDI .....	4
2.1 Introduction .....	4
2.2 Définition de l'EDI .....	4
2.3 Avantages et enjeux de l'EDI .....	6
3. Définition de l'EDIFACT .....	7

## *2<sup>ème</sup> Partie : Menaces, services et mécanismes de sécurité*

1. Introduction .....	12
2. Les menaces et les risques de la sécurité .....	13
3. Les solutions pour la sécurité : Les services de base et les technique ou les mécanismes de sécurité appropriés .....	15
3.1 Les services de base .....	15
3.1.1 Intégrité du contenu du message .....	15
3.1.2 L'authentification de l'origine du message .....	15
3.1.3 La non répudiation .....	15
a. La non répudiation de l'origine .....	15
b. La non répudiation avec preuve de réception .....	16
3.1.4 La confidentialité du contenu .....	16
3.1.5 Les corrélations entre les différents services de sécurité .....	16
3.2 Les techniques ou les mécanismes de sécurité .....	17
3.2.1 Le chiffrement .....	17
3.2.1.1 Chiffrement symétrique .....	18
Exemples d'algorithmes symétriques .....	20
1. le DES et ses variantes .....	20
1.1 DES .....	20
1.2 Variantes du DES .....	22
a. Triple DES .....	22
b. Double DES .....	23
1.3 Les modes .....	23
2. Blowfish .....	24
3. Comparaison des algorithmes symétriques .....	25
3.2.1.2 Chiffrement asymétrique .....	25
Exemples d'algorithmes asymétriques .....	27
1. le RSA .....	27
2. Le DSA .....	29
3. Comparaison des algorithmes asymétriques .....	29

3.2.1.3	Que dire de la sécurité des algorithmes cryptographiques ? .....	30
3.2.1.4	Que faut-il utiliser : un algorithme à clef secrète ou un algorithme à clef publique ? ....	30
3.2.2	La signature digitale .....	32
3.2.2.1	Création d'une signature digitale .....	32
a.	Définition de la fonction de Hachage .....	32
b.	Mécanisme de hachage .....	34
c.	Exemples de fonctions de Hachage .....	35
3.2.2.2	Vérification d'une signature digitale .....	36
3.2.2.3	Rôle de la signature digitale .....	37
3.2.2.4	Exigences pour la signature digitale .....	40
3.2.2.5	Gestion des clefs de signature .....	41
3.2.2.6	Les certificats .....	43

### *3<sup>ème</sup> Partie: Niveaux de Sécurité*

1.	Introduction .....	46
2.	Sécurité des messages X400 .....	48
2.1	Introduction.....	48
2.2	La structure X400 .....	50
3.	Comment sécuriser la structure EDIFACT .....	51
3.1	Préliminaire .....	51
3.2	Accord bilatéral / une tiers partie .....	51
3.3	Aspects pratiques .....	52
3.4	Procédure pour la construction d'une structure EDIFACT sécurisée .....	52
3.5	La séquence de services de sécurité d'une application .....	52
3.6	La sécurité au niveau du message .....	53
3.7	Principes d'usages .....	59
4.	Conclusion .....	60

### *4<sup>ème</sup> Partie : modèles conceptuels*

1.	Préface.....	61
2.	Modèle conceptuel SEC .....	62
2.1	Introduction .....	62
2.2	Conception de SEC .....	63
2.2.1	Présentation générale .....	63
2.2.2	Architecture de EDISEC .....	64
2.2.2.1	Les fonctions de EDISEC .....	64
2.2.2.1.1	Sécurité du message EDIFACT .....	64

2.2.2.1.2	<i>Vérification des messages de sécurité EDIFACT</i> .....	66
2.2.2.1.3	<i>Configuration</i> .....	67
2.2.2.1.4	<i>La gestion des clefs</i> .....	67
2.2.2.1.5	<i>Base de données des références des messages</i> .....	69
2.2.2.2	<i>Les services de sécurité qu'offre SEC</i> .....	70
2.2.2.3	<i>Les algorithmes cryptographiques appliqués</i> .....	70
2.3	<i>Conclusion</i> .....	70
3.	<i>Intégration de SEC au système EDI : EDISEC</i> .....	71
3.1	<i>Présentation générale</i> .....	71
3.2	<i>Intégration du système EDISEC</i> .....	72
4.	<i>Intégration de SEC au système de messagerie X400</i> .....	76
4.1	<i>Présentation générale</i> .....	76
4.2	<i>Structure de l'enveloppe du message X400</i> .....	77
<i>5<sup>ème</sup> Partie : Mise en œuvre</i>		
1.	<i>Environnement matériel et logiciel</i> .....	78
2.	<i>Implémentation des mécanismes de sécurité:</i>	
	<i>Implémentation de SEC</i> .....	79
	2.1 <i>Génération de la paire de clefs asymétriques RSA</i> .....	79
	2.2 <i>Hachage des messages</i> .....	80
	2.3 <i>Signature digitale</i> .....	81
	2.4 <i>Vérification de la signature digitale</i> .....	82
	2.5 <i>Encryptage des messages</i> .....	83
	2.6 <i>Décryptage des messages</i> .....	86
3.	<i>Intégration de EDISEC au prototype EDI400</i> .....	88
	3.1 <i>Présentation générale</i> .....	88
	3.2 <i>Présentation de EDISEC</i> .....	89
	3.3 <i>Traitement interne</i> .....	90
	3.4 <i>Fonctionnement du système EDISEC</i> .....	92

## *Conclusion*

## *Annexe A*

## *Annexe B*

## *Annexe C*

## *Glossaire*

## *Bibliographie*