

---

# Documentation SecurBdF

---

## SECURBDF V2

---

Protocole de sécurité de la  
Banque de France SecurBdF  
V2



Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page I

## Sommaire

<b><u>1</u></b>	<b><u>Contexte</u></b> .....	<b>1</b>
<b><u>2</u></b>	<b><u>Références</u></b> .....	<b>1</b>
<b><u>3</u></b>	<b><u>Cadre</u></b> .....	<b>2</b>
<b><u>4</u></b>	<b><u>Les services de sécurité de SecurBdF V2</u></b> .....	<b>3</b>
<b><u>4.1</u></b>	<b><u>Identification et authentification</u></b> .....	<b>3</b>
<b><u>4.2</u></b>	<b><u>Mécanismes : le scellement et le chiffrement</u></b> .....	<b>3</b>
4.2.1	<u>Intégrité des données / Scellement</u> .....	3
4.2.2	<u>Confidentialité des données / Chiffrement</u> .....	3
<b><u>4.3</u></b>	<b><u>Autres fonctions assurées par SecurBdF V2</u></b> .....	<b>3</b>
4.3.1	<u>La compression</u> .....	3
4.3.2	<u>Le transcodage des fichiers</u> .....	3
<b><u>5</u></b>	<b><u>Principe de fonctionnement de SecurBdF V2</u></b> .....	<b>4</b>
<b><u>6</u></b>	<b><u>Format du fichier à sécuriser</u></b> .....	<b>5</b>
<b><u>6.1</u></b>	<b><u>Format Fixe</u></b> .....	<b>5</b>
<b><u>6.2</u></b>	<b><u>Format Variable</u></b> .....	<b>5</b>
<b><u>6.3</u></b>	<b><u>Mode "Binaire"</u></b> .....	<b>5</b>
<b><u>7</u></b>	<b><u>Formatage du fichier « sécurisé »</u></b> .....	<b>6</b>
<b><u>7.1</u></b>	<b><u>Élimination des informations spécifiques</u></b> .....	<b>6</b>
7.1.1	<u>Fin de ligne</u> .....	6
7.1.2	<u>Fin de fichier</u> .....	6
<b><u>7.2</u></b>	<b><u>Transcodage (option)</u></b> .....	<b>6</b>
<b><u>7.3</u></b>	<b><u>Compression (option)</u></b> .....	<b>8</b>
7.3.1	<u>étape 1</u> .....	8
7.3.2	<u>étape 2</u> .....	9
7.3.3	<u>étape 3</u> .....	9
<b><u>7.4</u></b>	<b><u>Calcul du FID</u></b> .....	<b>9</b>
<b><u>7.5</u></b>	<b><u>Scellement du FID et du tampon</u></b> .....	<b>9</b>
<b><u>7.6</u></b>	<b><u>Adaptation du tampon (option chiffrement sans compression)</u></b> .....	<b>10</b>
7.6.1	<u>padding</u> .....	10
7.6.2	<u>Exemples :</u> .....	10
<b><u>7.7</u></b>	<b><u>Chiffrement du tampon (optionnel)</u></b> .....	<b>11</b>
<b><u>7.8</u></b>	<b><u>Décomposition en enregistrement de transport</u></b> .....	<b>11</b>
7.8.1	<u>Cas sans compression</u> .....	11
7.8.2	<u>Cas de la compression</u> .....	11
<b><u>7.9</u></b>	<b><u>Création des délimiteurs</u></b> .....	<b>12</b>
7.9.1	<u>Délimiteur préfixe (format de base)</u> .....	13
<b><u>7.10</u></b>	<b><u>Délimiteur suffixe (format de base)</u></b> .....	<b>16</b>
<b><u>7.11</u></b>	<b><u>Délimiteur de diffusion (format de base)</u></b> .....	<b>18</b>

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	<b>Date</b> 02/01/2003
		<b>Page</b> II

<b><u>7.12</u></b> Ajout des délimiteurs .....	<b>19</b>
7.12.1 Cas variable sans compression ou cas binaire.....	19
7.12.2 Cas fixe ou variable avec compression .....	19
7.12.3 Exemple de segmentation et de padding .....	20
<b><u>7.13</u></b> Format du fichier sécurisé.....	<b>20</b>
<b><u>8</u></b> <i>Mécanismes de sécurité</i> .....	<b>21</b>
<b><u>8.1</u></b> <i>Authentification</i> .....	<b>21</b>
<b><u>8.2</u></b> <i>Intégrité des données</i> .....	<b>21</b>
<b><u>8.3</u></b> <i>Intégrité des données en mode diffusion</i> .....	<b>22</b>
<b><u>8.4</u></b> <i>Confidentialité des données (hors compression)</i> .....	<b>23</b>
<b><u>8.5</u></b> <i>Confidentialité des données (avec compression)</i> .....	<b>24</b>
<b><u>A.1</u></b> <i>ANNEXE A : Engagement de confidentialité</i> .....	<b>25</b>

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	<b>Date</b> 02/01/2003
		<b>Page</b> 1 / 26

# 1 Contexte

---

Le présent document est le « Protocole de sécurité de la Banque de France SecurBdF V2 ». Il décrit la version 2 du protocole de sécurité de la Banque de France.

A partir de janvier 2004, un établissement qui échange avec la Banque de France des fichiers au format SecurBdF doit utiliser un logiciel conforme au protocole SecurBdF V2 détaillé dans ce document. Cet établissement peut soit acquérir le logiciel « SecurBdF Évolution » auprès de la Banque de France, soit développer ou faire développer un logiciel conforme au protocole SecurBdF V2.

Ce document technique est destiné aux personnes souhaitant comprendre le fonctionnement détaillé du protocole ou faisant partie d'une société tierce en charge de son implémentation.

# 2 Références

---

Le document « Service de sécurisation de fichiers : spécifications externes de SecurBdF V1.3 » décrit la version précédente du protocole. Il n'est pas indispensable à la compréhension du présent document.

Toutefois, il est rappelé aux sociétés tierces en charge du développement d'un logiciel compatible SecurBdF V2 qu'il est fortement conseillé d'être compatible en réception avec la version 1 du protocole.

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	<b>Date</b> 02/01/2003
		<b>Page</b> 2 / 26

## 3 Cadre

---

Le document se décompose en deux parties principales :

- La description du fichier dit « sécurisé » (mis au format du protocole SecurBdF V2);
- La description des algorithmes mis en œuvre pour calculer les éléments de sécurité liés aux services de sécurité activés.

La description du format de saisie des clés envoyées par le service RSI de la Banque de France aux établissements ne figure pas dans cette documentation publique. La société qui choisit de réaliser les développements de son propre logiciel de sécurisation devra envoyer à la Banque de France une demande de documentation supplémentaire accompagnée d'un engagement de confidentialité (cf. Annexe).

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 3 / 26

## 4 Les services de sécurité de SecurBdF V2

---

### 4.1 Identification et authentification

L'identification et l'authentification de l'émetteur sont le premier niveau de sécurité mis en œuvre automatiquement lors de la sécurisation d'un fichier suivant le protocole SecurBdF V2.

Ce premier niveau de sécurité permet de prouver que l'émetteur est bien celui qu'il prétend être.

### 4.2 Mécanismes : le scellement et le chiffrement

#### 4.2.1 INTÉGRITÉ DES DONNÉES / SCHELLEMENT

Le scellement du fichier permet :

- De garantir la conservation sans altération (accidentelle ou intentionnelle) des données pendant les opérations de traitement et de transmission du fichier ;
- D'assurer que les données n'ont pas été modifiées (par des personnes non autorisées) pendant la transmission du fichier sécurisé.

SecurBdF V2 offre en plus une option de diffusion : scellement d'un fichier en vue de l'envoyer à plusieurs destinataires. Cette option nécessite 2 clés pour chaque destinataire.

#### 4.2.2 CONFIDENTIALITÉ DES DONNÉES / CHIFFREMENT

Le chiffrement SecurBdF V2 permet :

- De transformer les données pour les rendre inaccessibles à toute personne non habilitée ;
- De conserver une donnée secrète vis-à-vis de tout le monde sauf du couple émetteur / récepteur des données (les seuls à posséder la clé secrète).

### 4.3 Autres fonctions assurées par SecurBdF V2

#### 4.3.1 LA COMPRESSION

La compression de fichier (offerte en option par le protocole SecurBdF V2) est destinée à réduire la taille du fichier avant de le sécuriser. Cela permet de réduire la durée du transfert et de gagner en performances pour les fichiers de grande taille.

#### 4.3.2 LE TRANSCODAGE DES FICHIERS

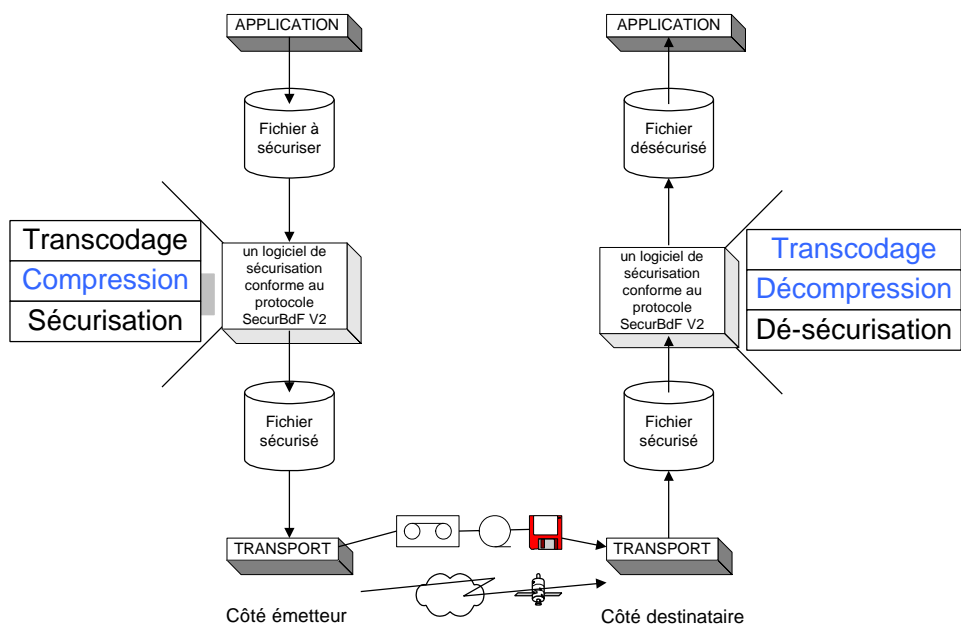
Selon les plates-formes informatiques, le codage des caractères peut être différent :

- ASCII pour les plates-formes UNIX et WINDOWS ;
- EBCDIC pour les plates-formes AS400, MVS et GCOS7.

Le choix de l'un ou l'autre de ces codages dépend des échanges de fichiers avec la Banque de France.

## 5 Principe de fonctionnement de SecurBdF V2

Le principe général de fonctionnement du protocole s'illustre par le schéma suivant :



Les étapes de sécurisation à réaliser sont les suivantes :

- Lecture du fichier à sécuriser,
- Suppression éventuelle des sauts de lignes et de la marque de fin de fichier,
- Transcodage,
- Structuration des données si compression,
- Calcul du FID ("File IDentification"),
- Scellement du FID et éventuellement des données structurées,
- Si chiffrement sans compression, complément à 8 des enregistrements,
- Chiffrement s'il est activé,
- Décomposition en enregistrements,
- Création des délimiteurs (préfixe et suffixe) avec leur éventuelle décomposition sur plusieurs enregistrements,
- Ajout des délimiteurs.

Les étapes de dé-sécurisation à réaliser sont les suivantes :

- Lecture et retrait des délimiteurs (préfixe, suffixe de diffusion éventuel, suffixe normal),
- Retrait des informations d'enregistrement,
- Déchiffrement si le chiffrement était activé,
- Retrait des compléments à 8 si chiffrement sans compression,
- Vérification du scellement du FID et éventuellement des données structurées,
- Vérification si besoin du scellement de diffusion
- Décompression,
- Transcodage,
- Rajout éventuel des sauts de lignes et de la marque de fin de fichier.

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 5 / 26

## 6 Format du fichier à sécuriser

---

On rappelle que même sur les plates-formes non structurées (ex. Windows, Unix), chaque fichier à sécuriser est assimilé à une succession d'enregistrements. Sous Windows, un enregistrement est constitué d'une ligne séparée par les deux octets #0A et #0D (« CRLF »).

La sécurisation considère 3 types de fichiers :

- Format fixe ;
- Format variable ;
- Mode "binaire".

### 6.1 Format Fixe

Ce sont les fichiers dont l'ensemble des enregistrements ont la même taille.

Cette taille doit être comprise entre 14 octets et 32704 octets.

### 6.2 Format Variable

Ce sont les fichiers dont les enregistrements n'ont pas forcément la même taille.

Le plus petit enregistrement doit avoir une longueur d'au moins 1 octet.

Le plus grand enregistrement doit avoir une longueur d'au plus 32704 octets.

Dans le cas d'une sécurisation avec compression, la taille du fichier à sécuriser (ou un majorant de celle-ci) devra être utilisée pour structurer le fichier sécurisé.

### 6.3 Mode "Binaire"

Ce mode n'est pris en compte que sur les plates-formes Unix ou Windows.

Il permet de sécuriser n'importe quel fichier (textes, programmes, images, base de données, etc.). **Il ne s'utilise que dans le cadre d'échanges entre plates-formes ayant un format binaire compatible.** Le fichier d'entrée est pris dans son entier y compris les «*Fin de ligne*» et «*Fin de fichier*», s'il y en a, qui ne sont pas éliminés.

La taille maximum de fichier qui peut être sécurisé via le protocole SecurBdF étant codée sur 15 bits, le fichier binaire sera considéré comme un fichier d'entrée dont tous les enregistrements de données auront une taille de 32704 octets, sauf le dernier qui aura la taille non nulle restante (taille du fichier modulo 32704).

Les délimiteurs seront laissés à leur taille de base.

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 6 / 26

## 7 Formatage du fichier « sécurisé »

Quelles que soient les options de sécurisation choisies, la structure du fichier « sécurisé » (en sortie d'émission) diffère de celle du fichier en entrée. Cette modification de structure (nombre d'enregistrements, longueur d'enregistrement) est nécessaire notamment pour transmettre les paramètres de sécurité et pour permettre les échanges de données entre matériels hétérogènes (indication de la taille de chaque bloc de données sur deux octets en tête de chaque enregistrement). Le format du fichier « sécurisé » est un format pivot indépendant des plates-formes utilisées.

Les chapitres suivants indiquent les différentes transformations à opérer pour formater le fichier sécurisé. Les différentes transformations seront appliquées au travers d'un tampon.

### 7.1 Élimination des informations spécifiques

#### 7.1.1 FIN DE LIGNE

La séquence d'octets, spécifique à la plate-forme émettrice, utilisée pour indiquer les fins de lignes (fin d'enregistrement) est éliminée du tampon contenant les données à sécuriser (sauf en mode binaire). Cette séquence peut être vide.

Sur la plate-forme réceptrice, la séquence de fin de ligne propre à cette dernière est re-générée selon le système cible. Dans le cas d'un système structuré (ex. MVS, GCOS7, AS400, TANDEM), cela peut consister en la création d'une enveloppe adéquate pour contenir le fichier.

#### 7.1.2 FIN DE FICHIER

Certaines applications dans le monde ASCII utilisent un octet (#1A) pour indiquer la fin de fichier. Cette indication doit être retirée du tampon d'émission.

En réception, l'application à qui sont destinées les données peut elle aussi nécessiter cette indication de fin de fichier (un champ du préfixe peut être utilisé pour véhiculer cette information si le destinataire le demande).

### 7.2 Transcodage (option)

Le transcodage ne s'applique pas au fichier à sécuriser en mode binaire.

Le logiciel implémentant SecurBdF V2 opère, si besoin, un transcodage entre ASCII et EBCDIC suivant la table de transcodage donnée ci-après. Le logiciel doit aussi pouvoir prendre en compte une modification de cette table pour les besoins propres d'une application.

La gestion du transcodage inclut :

- Le transcodage ASCII-ASCII en émission et en réception ;
- Le transcodage EBCDIC-EBCDIC en émission et en réception ;
- Le transcodage ASCII-EBCDIC en émission et en réception (réception d'un fichier ASCII sur une plate-forme en EBCDIC) ;
- Le transcodage EBCDIC-ASCII en émission et en réception (réception EBCDIC d'un fichier sur une plate-forme en ASCII).

Les Tables de correspondance par défaut sont les suivantes :

EBCDIC	Correspondance [EBCDIC->ASCII]															
	#XY	#X0	#X1	#X2	#X3	#X4	#X5	#X6	#X7	#X8	#X9	#XA	#XB	#XC	#XD	#XE
#0Y	=	=	=	=	#9C	#09	#86	#7F	#97	#8D	#8E	=	=	=	=	=
#1Y	=	=	=	=	#9D	#85	#08	#87	#18	#19	#92	#8F	=	=	=	=
#2Y	#80	#81	#82	#83	#84	#0A	#17	#1B	#88	#89	#8A	#8B	#8C	#05	#06	#07
#3Y	#90	#91	#16	#93	#94	#95	#96	#04	#98	#99	#9A	#9B	#14	#15	#9E	#1A
#4Y	#20	#A0	#A1	#A2	#A3	#A4	#A5	#A6	#A7	#A8	#5B	#2E	#3C	#28	#2B	#21
#5Y	#26	#A9	#AA	#AB	#AC	#AD	#AE	#AF	#B0	#B1	#5D	#24	#2A	#29	#3B	#5E
#6Y	#2D	#2F	#B2	#B3	#B4	#B5	#B6	#B7	#B8	#B9	#7C	#2C	#25	#5F	#3E	#3F
#7Y	#BA	#BB	#BC	#BD	#BE	#BF	#C0	#C1	#C2	#60	#3A	#23	#40	#27	#3D	#22
#8Y	#C3	#61	#62	#63	#64	#65	#66	#67	#68	#69	#C4	#C5	#C6	#C7	#C8	#C9
#9Y	#CA	#6A	#6B	#6C	#6D	#6E	#6F	#70	#71	#72	#CB	#CC	#CD	#CE	#CF	#D0
#AY	#D1	#7E	#73	#74	#75	#76	#77	#78	#79	#7A	#D2	#D3	#D4	#D5	#D6	#D7
#BY	#D8	#D9	#DA	#DB	#DC	#DD	#DE	#DF	#E0	#E1	#E2	#E3	#E4	#E5	#E6	#E7
#CY	#7B	#41	#42	#43	#44	#45	#46	#47	#48	#49	#E8	#E9	#EA	#EB	#EC	#ED
#DY	#7D	#4A	#4B	#4C	#4D	#4E	#4F	#50	#51	#52	#EE	#EF	#FA	#FB	#FC	#FD
#EY	#5C	#9F	#53	#54	#55	#56	#57	#58	#59	#5A	#F4	#F5	#F6	#F7	#F8	#F9
#FY	#30	#31	#32	#33	#34	#35	#36	#37	#38	#39	=	=	=	=	=	=

(= indique les valeurs inchangées)

ASCII	Correspondance [ASCII->EBCDIC]															
	#XY	#X0	#X1	#X2	#X3	#X4	#X5	#X6	#X7	#X8	#X9	#XA	#XB	#XC	#XD	#XE
#0Y	=	=	=	=	#37	#2D	#2E	#2F	#16	#05	#25	=	=	=	=	=
#1Y	=	=	=	=	#3C	#3D	#32	#26	#18	#19	#3F	#27	=	=	=	=
#2Y	#40	#4F	#7F	#7B	#5B	#6C	#50	#7D	#4D	#5D	#5C	#4E	#6B	#60	#4B	#61
#3Y	#F0	#F1	#F2	#F3	#F4	#F5	#F6	#F7	#F8	#F9	#7A	#5E	#4C	#7E	#6E	#6F
#4Y	#7C	#C1	#C2	#C3	#C4	#C5	#C6	#C7	#C8	#C9	#D1	#D2	#D3	#D4	#D5	#D6
#5Y	#D7	#D8	#D9	#E2	#E3	#E4	#E5	#E6	#E7	#E8	#E9	#4A	#E0	#5A	#5F	#6D
#6Y	#79	#81	#82	#83	#84	#85	#86	#87	#88	#89	#91	#92	#93	#94	#95	#96
#7Y	#97	#98	#99	#A2	#A3	#A4	#A5	#A6	#A7	#A8	#A9	#C0	#6A	#D0	#A1	#07
#8Y	#20	#21	#22	#23	#24	#15	#06	#17	#28	#29	#2A	#2B	#2C	#09	#0A	#1B
#9Y	#30	#31	#1A	#33	#34	#35	#36	#08	#38	#39	#3A	#3B	#04	#14	#3E	#E1
#AY	#41	#42	#43	#44	#45	#46	#47	#48	#49	#51	#52	#53	#54	#55	#56	#57
#BY	#58	#59	#62	#63	#64	#65	#66	#67	#68	#69	#70	#71	#72	#73	#74	#75
#CY	#76	#77	#78	#80	#8A	#8B	#8C	#8D	#8E	#8F	#90	#9A	#9B	#9C	#9D	#9E
#DY	#9F	#A0	#AA	#AB	#AC	#AD	#AE	#AF	#B0	#B1	#B2	#B3	#B4	#B5	#B6	#B7
#EY	#B8	#B9	#BA	#BB	#BC	#BD	#BE	#BF	#CA	#CB	#CC	#CD	#CE	#CF	#DA	#DB
#FY	#DC	#DD	#DE	#DF	#EA	#EB	#EC	#ED	#EE	#EF	=	=	=	=	=	=

(= indique les valeurs inchangées)

EBCDIC	Correspondance [EBCDIC->EBCDIC]															
	#XY	#X0	#X1	#X2	#X3	#X4	#X5	#X6	#X7	#X8	#X9	#XA	#XB	#XC	#XD	#XE
#0Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#1Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#2Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#3Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#4Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#5Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#6Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#7Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#8Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#9Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#AY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#BY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#CY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#DY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#EY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#FY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=

(= indique les valeurs inchangées)

ASCII	Correspondance [ASCII->ASCII]																
	#XY	#X0	#X1	#X2	#X3	#X4	#X5	#X6	#X7	#X8	#X9	#XA	#XB	#XC	#XD	#XE	#XF
#0Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#1Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#2Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#3Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#4Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#5Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#6Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#7Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#8Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#9Y	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#AY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#BY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#CY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#DY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#EY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
#FY	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=

(= indique les valeurs inchangées)

**Remarque :** par défaut, il n'y a pas de transcodage ASCII-ASCII et EBCDIC-EBCDIC. Les valeurs restent identiques à elle-même sauf indication contraire donnée par une spécificité d'une plate-forme (ex. établissement ayant un système d'exploitation n'utilisant pas l'alphabet français).

## 7.3 Compression (option)

La compression est de type mixte (Horizontal/Vertical), elle ne peut s'appliquer que sur des fichiers d'enregistrements au format fixe ou variable. Les fichiers à sécuriser en mode binaire ne sont donc pas compressibles.

Si la compression est activée, les données compressées issues d'un enregistrement sont mises à la suite les unes des autres, précédées de la longueur de l'enregistrement compressé.

Le fichier sécurisé compressé aura donc une sous-structure spécifique. Au final après l'opération d'ajout des délimiteurs, les enregistrements auront tous la même taille y compris les délimiteurs, cette taille sera celle du plus grand enregistrement + 2 octets (longueur du bloc).

Nous rappelons que même si cela est très peu probable au vu des types de données échangées, un enregistrement « compressé » peut être plus grand que l'enregistrement initial. Si la compression est demandée, le fichier doit être transmis compressé même si la compression est « négative ».

Pour faciliter la compréhension de la compression, les différentes actions sont découpées en étapes.

### 7.3.1 ÉTAPE 1

Chaque enregistrement est compressé en utilisant une compression mixte.

Enreg1\_compressé = Compression(Enreg1)

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 9 / 26

### 7.3.2 ÉTAPE 2

A l'issue de la fonction de compression, on aura un tampon virtuel contenant l'ensemble du fichier (comprimé) sous la forme suivante :

□□Enreg1_compressé...□□Enreg2_compressé...□□...□□EnregN_compressé...
--

□□ représente les deux octets du compteur de longueur de l'enregistrement compressé

### 7.3.3 ÉTAPE 3

Deux cas se présentent :

- Le chiffrement est activé en plus de la compression ;
- Le chiffrement n'est pas activé.

Le tampon est alors suivant l'un de ces cas :

- Complété par un padding en multiple de huit en fin de tampon ;
- Conservé à l'identique.

Suivant les options, le tampon subira d'autres traitements (scellement, chiffrement).

## 7.4 Calcul du FID

Le "File IDentification" est calculé à partir de la concaténation des champs textes suivants transcodés si besoin en ASCII ou EBCDIC comme les données à sécuriser (cf. 7.2 Transcodage (option)):

- Type de fichier (champ 7 du préfixe, 8 octets) ;
- Nom de fichier (champ 8 du préfixe, 14 octets) ;
- Date et heure (caractères AAMMJJHHMMSS, 12 octets). En émission date et heure de la sécurisation. En réception, re - codage en caractères des 6 premiers octets du champ 9 du préfixe) ;
- Identifiant Émetteur (champ 4 du préfixe, 24 octets) ;
- Identifiant Récepteur (champ 6 du préfixe, 24 octets).

## 7.5 Scellement du FID et du tampon

En émission, il convient de calculer le sceau :

Le FID est scellé par un MAC DES (cf. 8.1 Authentification),

puis si besoin le tampon est scellé (cf. 8.2 Intégrité des données).

En réception, le sceau doit être vérifié, et le "slot" du destinataire doit être également vérifié dans le cas d'un fichier en diffusion (cf. 8.3 Intégrité des données en mode diffusion).

## 7.6 Adaptation du tampon (option chiffrement sans compression)

### 7.6.1 PADDING

On rappelle que cette adaptation ne s'applique pas si la compression est activée (cf. 7.3 Compression).

Le principe de l'algorithme **DES** est de travailler par groupes de 8 octets. Dans le cas d'un chiffrement sans compression, la compatibilité avec la longueur des enregistrements réalisés par un protocole SecurBdF V1 a été conservée.

Les données issues de chaque enregistrement seront complétées («padding») au multiple de 8 supérieur. Le logiciel doit ajouter 8 octets même si la taille est déjà multiple de 8 pour conserver l'homogénéité du traitement de réception.

$$n = \text{nombre d'octets de padding} = (8 - (\text{longueur d'enregistrement} \text{ MODULO } 8))$$

*MODULO* 8 donne le reste de la division par 8.

Le padding est effectué sur le tampon avec des zéros binaires (#00) pour les (n-1) premiers octets, le dernier octet aura comme valeur hexadécimale #0(n-1).

Dans le cas d'une sécurisation vers un fichier au format fixe, cette longueur de padding n est à noter car elle sera utilisée dans le padding du préfixe (dernier octet de padding).

Pour un fichier sécurisé en mode "binaire", la longueur d'enregistrement est égale à 32704 octets sauf pour le dernier enregistrement qui prend la taille restante (longueur du fichier modulo 32704).

### 7.6.2 EXEMPLES :

#### 7.6.2.1 ENREGISTEMENT DE TAILLE 118

Pour un enregistrement de **118** caractères (*hors séquence de fin de ligne*), **2** octets seront ajoutés pour atteindre **120** (8 × 15) ; le premier octet vaudra #00, le second #01.

Le tampon est considéré comme une suite d'enregistrements de 118 caractères (les fins de lignes ont déjà été supprimées) :

Enreg.....(118 caractères) .....	
Enreg.....(118 caractères) .....	
Enreg.....(118 caractères) .....	
...	

Enregistrement paddé :

Enreg.....(118 caractères) .....	#00#01
Enreg.....(118 caractères) .....	#00#01
Enreg.....(118 caractères) .....	#00#01
....	

#### 7.6.2.2 ENREGISTEMENT DE TAILLE 240

Pour une taille de **240** (déjà multiple de 8) il y aura **8** octets de padding ; les 7 premiers seront #00 et le dernier #07 avant chiffrement.

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 11 / 26

## 7.7 Chiffrement du tampon (optionnel)

Si le chiffrement est activé, la taille du tampon est maintenant un multiple de 8 octets. Le padding a été réalisé soit lors de la structuration de la compression soit pour le chiffrement sans compression.

Le chiffrement est réalisé en DES ou 3DES suivant l'option choisie (cf. 8.4).

## 7.8 Décomposition en enregistrements de transport

### 7.8.1 CAS SANS COMPRESSION

Le tampon est dorénavant dit « sécurisé », sa structure est la suivante :

```
Enreg1_SecuriséEnreg2_Securisé...EnregN_Securisé..
```

Chaque enregistrement va être précédé par sa longueur codée sur 2 octets. Ce qui donne :

```
□□Enreg1_Securisé□□Enreg2_Securisé... □□EnregN_Securisé..
```

□□ représente les deux octets du compteur de longueur de l'enregistrement

Si on compare avec les enregistrements avant sécurisation, les différentes valeurs du compteur sont les suivantes :

- Sans chiffrement : égal à la longueur de l'enregistrement initial.
- Avec chiffrement : égal à la longueur de l'enregistrement initial + (8 - (lg MODULO 8)).

On appelle enregistrement de transport les données □□Enreg\_Securisé.

Chaque enregistrement de transport a une longueur égale à sa longueur plus les 2 octets de longueur du compteur.

### 7.8.2 CAS DE LA COMPRESSION

Le tampon est dorénavant dit sécurisé, il n'a plus de structure, c'est une suite d'octets :

```
Suite_octets_sans_structure
```

Le tampon qui a une longueur lg\_tp va être structuré sur des blocs d'octets de longueur constante.

Soit lg\_ini cette longueur.

- lg\_ini = longueur de l'enregistrement initial pour un fichier d'entrée en taille fixe  
longueur du plus grand enregistrement initial pour un fichier en taille variable

Dans un premier temps, une longueur va être introduite pour déterminer la frontière entre les octets utiles et les blancs de padding.

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 12 / 26

La suite d'octet devient alors (Suite\_octets\_restants peut être vide) :

```
Suite_octets_multiple_de_lg_ini■■Suite_octets_restants
```

■■ représente les deux octets du reste lg\_tp par lg\_ini

Puis, on complète le tampon par des blancs (#20 en ASCII et #40 en EBCDIC) pour obtenir un multiple de lg\_ini. Si la suite précédente est déjà un multiple de lg\_ini, on rajoute lg\_ini blancs.

```
Suite_octets_multiple_de_lg_ini■■Suite_octets_restantsSuite_de_blancs
```

Enfin, on insère la longueur lg\_ini à intervalle régulier, il faut cependant noter que la suite finale (■■Suite\_octets\_restantsSuite\_de\_blancs) peut être de taille supérieure à lg\_ini. De ce fait le tampon final a donc deux formes possibles :

- forme 1 :

```
□□bloc1_octets□□bloc2_octets...☒□■■Suite_octets_restantsSuite_de_blancs
```

- forme 2 :

```
□□bloc1_octets□□bloc2_octets...☒□■■Suite_octets_restantsPart1_blancs☒□Part2_blancs
```

□□ représente les deux octets du compteur de longueur valant lg\_ini

☒□ identique au précédent mais avec le bit de poids fort du premier octet armé à un

■■ représente les deux octets du reste lg\_tp par lg\_ini

On appelle enregistrement de transport les données □□bloc\_données ou ☒□ bloc\_données

Chaque enregistrement de transport a une longueur égale à lg\_ini + 2 octets.

## 7.9 Création des délimiteurs

Au cours de la sécurisation, des données supplémentaires, appelées délimiteurs, sont ajoutées au fichier à « sécuriser » ou retirées du fichier à « dé-sécuriser ».

Il y a trois types de délimiteurs :

- Le préfixe placé au début du fichier (obligatoire) ;
- Le suffixe placé à la fin du fichier (obligatoire) ;
- Le délimiteur de diffusion placé juste avant le suffixe (existe seulement quand la diffusion est activée par la Banque de France).

Ils contiennent les paramètres de sécurité qui permettront au destinataire d'effectuer la réception des données.

Les 3 chapitres suivants décrivent le contenu des délimiteurs dans leur format de base, c'est à dire, sans segmentation et sans padding.

### 7.9.1 DÉLIMITEUR PRÉFIXE (FORMAT DE BASE)

	CHAMPS	Type	Position de base	Longueur
0	Compteur longueur	B	1	2
1	Code enregistrement	B	3	2
2	Version du délimiteur	B	5	2
3	Type de codage du fichier sécurisé	B	7	1
4	Identificateur émetteur	C	8	24
5	Références complémentaires client	C	32	24
6	Identificateur récepteur	C	56	24
7	Type de fichier	C	80	8
8	Nom du fichier	C	88	14
9	Date et heure de création/format-longueur	C	102	12
10	Type de scellement	C	114	4
11	Type de chiffrement	C	118	4
12	Éléments de scellement	C	122	8
	Clé de session K1	B	130	8
	Vecteur d'initialisation IV1	B	138	8
13	Éléments de chiffrement	C	146	8
	Clé de session K2	B	154	8
	Vecteur d'initialisation IV2	B	162	8
<b>TOTAL</b>				169

Longueur hors compteur de longueur = 167 octets.

B = binaire. C = caractère (transcodé si besoin).

Les valeurs binaires sont spécifiées en base hexadécimale et précédées du caractère # (dièse). Les valeurs de type caractère sont encadrées par le caractère " (double cote).

Champ 0	Compteur longueur
Sur deux octets, en base 256, indique la longueur de l'enregistrement qui suit.	
Champ 1	Code enregistrement
1 <sup>er</sup> octet	#00 (hexadécimal) constante caractérisant le préfixe.
2 <sup>ème</sup> octet	<ul style="list-style-type: none"> <li>• #11 en format variable ou en mode binaire</li> <li>• en format fixe : (cf. Cas fixe ou variable avec compression). <ul style="list-style-type: none"> <li>◇ premier demi-octet x : rang du segment (de #1y à #Fy)</li> <li>◇ deuxième demi-octet y : nombre total de segments (de #x1 à #xF)</li> </ul> </li> </ul> <p><u>Remarque</u> : en format fixe, lorsque la longueur de l'enregistrement est supérieure ou égale à celle du délimiteur, il n'y a qu'un segment. En conséquence, le rang du segment vaut 1, et le nombre total de segments est 1. La valeur du 2<sup>ème</sup> octet est dans ce cas aussi #11.</p>
Champ 2	Version du délimiteur
#02#00 constante.	

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 14 / 26

Champ 3	Type de codage du fichier sécurisé
<p><b>Premier demi octet :</b> indique la nécessité d'ajouter au fichier dé-sécurisé une marque de fin de fichier (#1A), dans le cas d'un fichier ASCII uniquement et indique la compression</p> <ul style="list-style-type: none"> <li>• #bbb0 absence de marque de fin de fichier (#1A)</li> <li>• #bbb1 présence de marque de fin de fichier (#1A) <ul style="list-style-type: none"> <li>◊ bbb=000 sans compression</li> <li>◊ bbb=011 compression HV</li> </ul> </li> </ul> <p><b>Deuxième demi octet :</b></p> <ul style="list-style-type: none"> <li>• #x0 = ASCII</li> <li>• #x1 = EBCDIC</li> <li>• #x2 = BINAIRE (le premier demi - octet est nul dans ce cas).</li> </ul>	

Champ 4	Identificateur émetteur
<p>Les 3 premiers caractères sont obligatoirement :</p> <ul style="list-style-type: none"> <li>• "ZBF" pour la Banque de France ou</li> <li>• "ZZZ" pour un autre établissement</li> </ul> <p>suivis de la codification de l'émetteur, complétés éventuellement par des espaces. Il s'agit ici de l'identifiant complet (i.e. complété avec indicateur de génération de clé)</p>	

Champ 5	Références complémentaires client
Champ facultatif (peut être vide) complété par des espaces.	

Champ 6	Identificateur récepteur
<p>Les 3 premiers caractères sont obligatoirement :</p> <ul style="list-style-type: none"> <li>• "ZBF" pour la Banque de France ou</li> <li>• "ZZZ" pour un autre établissement</li> </ul> <p>suivis de la codification du récepteur(destinataire), complétés éventuellement par des espaces. Il s'agit ici de l'identifiant complet (i.e. complété avec indicateur de génération de clé)</p>	

Champ 7	Type de fichier
<p><b>1<sup>er</sup> caractère :</b> convention de transfert</p> <ul style="list-style-type: none"> <li>• "4" pour les conventions CFONB.</li> <li>• "0" pour les autres conventions.</li> </ul> <p><b>7 caractères suivants :</b> type de fichier ou remplis d'espaces si inutilisé.</p>	

Champ 8	Nom du fichier
<p>14 caractères :</p> <p>2 premiers caractères : "00" (zéro-zéro).</p> <p>12 suivants : nom du fichier.</p> <p>Rappel : ce n'est pas forcément le nom physique du fichier. Il s'agit d'un nom de convention entre les deux interlocuteurs.</p>	

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 15 / 26

Champ 9	Date et heure de création/format-longueur
<p>Indique la date (année, mois et jour) et l'heure (heures, minutes et secondes) de la sécurisation chez l'émetteur (sous la forme de 12 digits #AA #MM #JJ #HH #MM #SS) et indique sous la forme de 12 digits la longueur du fichier et le format du fichier avant sécurisation (#FL #LL #LL #LL #LL #LL) avec F à 0 pour fixe et 1 pour variable</p> <p>Ces dernières informations seront aussi codées en 12 digits avec un padding à zéro à gauche (ex. #F0 #00 #00 #01 #23 #45 pour un fichier de 12 345 octets, F sera soit 0 pour le format fixe soit 1 si le fichier initial a des enregistrements de taille variable).</p>	

Champ 10	Type de scellement
<p><b>1<sup>er</sup> caractère :</b></p> <ul style="list-style-type: none"> <li>"0" : pas de scellement du fichier (seulement du FID)</li> <li>"1" : scellement du fichier et du FID activé.</li> </ul> <p><b>2<sup>ème</sup> caractère :</b></p> <ul style="list-style-type: none"> <li>"1" = usage d'un MAC DES sur le condensé du fichier hors séparateurs (MD5)</li> </ul> <p><b>3<sup>ème</sup> caractère :</b></p> <ul style="list-style-type: none"> <li>"2" = transmission du sceau final uniquement.</li> <li>"9" = transmission d'un sceau final et diffusion d'un sceau chiffré par correspondant (valeur de champ réservée BdF).</li> </ul> <p><b>4<sup>ème</sup> caractère :</b></p> <p>"3" = transfert des éléments de scellement chiffrés par le 3DES.</p>	

Champ 11	Type de chiffrement
<p><b>1<sup>er</sup> caractère :</b></p> <ul style="list-style-type: none"> <li>"0" : pas de chiffrement.</li> <li>"1" : chiffrement activé.</li> </ul> <p><b>2<sup>ème</sup> caractère :</b></p> <ul style="list-style-type: none"> <li>"1" = usage de l'algorithme DES.</li> <li>"2" = usage de l'algorithme triple DES.</li> </ul> <p><b>3<sup>ème</sup> caractère :</b></p> <p>"1" = mode de chiffrement CBC.</p> <p><b>4<sup>ème</sup> caractère :</b></p> <p>"2" = transfert des éléments de chiffrement chiffrés par le triple DES.</p>	

Champ 12	Éléments de scellement
KEK	Champ égal à " <b>KEK123</b> " complété par 2 blancs
Clé de session K1	Valeur sur 8 octets de la clé de session pour le scellement (K1), générée au moment de la sécurisation et chiffrée avec la clé définie dans la zone précédente.
Vecteur d'initialisation IV1	Les 8 derniers octets contiennent une valeur d'initialisation aléatoire chiffrée par la KEK.

Champ 13	Éléments de chiffrement
KEK	Identique au champ 12. Champ égal à " <b>KEK123</b> " complété par 2 blancs.
Clé de session K2	Valeur, sur 8 octets, <ul style="list-style-type: none"> <li>- Si chiffrement DES : de la clé de session pour le chiffrement (K2), générée au moment de la sécurisation et chiffrée avec la clé définie dans la zone précédente.</li> <li>- Si chiffrement 3DES : première partie de la clé 3DES.</li> </ul> (La deuxième partie est égale à K1 indiquée dans le champ 12 La troisième partie est égale à IV1 (sans parité) indiqué dans le champ 12)
Vecteur d'initialisation IV2	Valeur d'initialisation, chiffrée par la KEK, servant de base au chiffrement.

## 7.10 Délimiteur suffixe (format de base)

	CHAMPS	Type	Position de base	Longueur
0	Compteur longueur (bit de poids fort à 1 en V2)	B	1	2
1	Code enregistrement	B	3	2
2	Bloc de contrôle de clé	B	5	2
3	Type de codage du fichier sécurisé	B	7	1
4	Identificateur émetteur	C	8	24
5	Références complémentaires client	C	32	24
6	Identificateur récepteur	C	56	24
7	Type de fichier	C	80	8
8	Nom du fichier	C	88	14
9	Date et heure de création	B	102	12
10	Sceau	B	114	8
<b>TOTAL</b>				121

Longueur hors compteur de longueur = 119 octets.

B = binaire. C = caractère (transcodé si besoin).

Les valeurs binaires sont spécifiées en base hexadécimale et précédées du caractère # (dièse), Les valeurs de type caractère sont encadrées par le caractère " (double cote).

Champ 0	Compteur longueur
Sur deux octets, en base 256, indique la longueur de l'enregistrement qui suit (le bit de poids fort est armé en V2). Le bit de poids fort du premier octet est à un.	

Champ 1	Code enregistrement
<p><b>1<sup>er</sup> octet :</b> #FF (hexadécimal) constante caractérisant le suffixe.</p> <p><b>2<sup>ème</sup> octet :</b></p> <ul style="list-style-type: none"> <li>• #11 en mode binaire</li> <li>• en format fixe ou variable : (cf. Cas fixe ou variable avec compression). <ul style="list-style-type: none"> <li>◇ Premier demi-octet : rang du segment (de #1y à #Fy)</li> <li>◇ Deuxième demi-octet : nombre total de segments (de #x1 à #xF)</li> </ul> </li> </ul> <p><u>Remarque</u> : en format fixe, lorsque la longueur de l'enregistrement est supérieure ou égale à celle du délimiteur, il n'y a qu'un segment. En conséquence, le rang du segment vaut 1, et le nombre total de segment est 1. La valeur du 2<sup>ème</sup> octet est dans ce cas aussi #11.</p>	

Champ 2	Bloc de contrôle de clé
<p>Ce bloc binaire de deux octets permet de distinguer les erreurs dues à un sceau fraudé des erreurs dues à des clés déphasées. Il est obtenu en prenant l'octet de poids fort suivi de l'octet de poids faible du bloc de 8 octets R résultant du calcul suivant :</p> $A = (64 \times 3) \text{DES}(\text{Permutation de KEK choisie}, \langle K1 \rangle) \text{ [lg A = 64 bits]}$ $B = \text{DES en mode CBC (A, IV1}   \langle \text{KEK123} \rangle) \text{ [lg B = 192 bits]}$ $R = (32 \times 3) \text{DES}(B, \langle K1 \oplus \text{IV1} \rangle) \text{ [lg R = 64 bits]}$ <p>avec les notations :</p> <p>DES en mode CBC (clé, vecteur   bloc) ;</p> <p>3DES (clé, bloc)</p> <p>(nx3DES) pour 3DES<sup>N</sup></p>	

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 17 / 26

Champ 3	Type de codage du fichier sécurisé
<p><b>Premier demi octet :</b> indique la nécessité d'ajouter au fichier dé-sécurisé une marque de fin de fichier (#1A), dans le cas d'un fichier ASCII uniquement et indique la compression</p> <p>#bbb0 absence de marque de fin de fichier (#1A) #bbb1 présence de marque de fin de fichier (#1A)</p> <ul style="list-style-type: none"> <li>◇ bbb=000 sans compression</li> <li>◇ bbb=011 compression HV</li> </ul> <p><b>Deuxième demi octet :</b></p> <p>#x0 = ASCII #x1 = EBCDIC #x2 = BINAIRE (le premier demi - octet est nul dans ce cas).</p>	

Champ 4	Identificateur émetteur
<p>Les 3 premiers caractères sont obligatoirement :</p> <p><b>"ZBF"</b> pour la Banque de France ou <b>"ZZZ"</b> pour un autre établissement</p> <p>suivis de la codification de l'émetteur, complétés éventuellement par des espaces. Il s'agit ici de l'identifiant complet (i.e. complété avec indicateur de génération de clé)</p>	

Champ 5	Références complémentaires client
Champ facultatif	

Champ 6	Identificateur récepteur
<p>Les 3 premiers caractères sont obligatoirement :</p> <p><b>"ZBF"</b> pour la Banque de France ou <b>"ZZZ"</b> pour un autre établissement</p> <p>suivis de la codification du récepteur(destinataire), complétés éventuellement par des espaces.</p>	

Champ 7	Type de fichier
<p><b>1<sup>er</sup> caractère :</b> convention de transfert</p> <p><b>"4"</b> pour les conventions CFONB. <b>"0"</b> pour les autres conventions.</p> <p><b>7 caractères suivants :</b> type de fichier ou remplis d'espaces si inutilisé.</p>	

Champ 8	Nom du fichier
<p>14 caractères :</p> <p>2 premiers caractères : <b>"00"</b> (zéro-zéro). 12 suivants : nom du fichier.</p> <p>Rappel : ce n'est pas forcément le nom physique du fichier. Il s'agit d'un nom de convention entre les deux interlocuteurs.</p>	

Champ 9	Date et heure de création
<p>Indique la date (année, mois et jour) et l'heure (heures, minutes et secondes) de la sécurisation chez l'émetteur (sous la forme de 12 digits #AA #MM #JJ #HH #MM #SS) et indique sous la forme de 12 digits la longueur du fichier et le format du fichier avant sécurisation (#FL #LL #LL #LL #LL #LL #LL) avec F à 0 pour fixe et 1 pour variable</p>	

Champ 10	Sceau
<p>Sceau d'authentification et de scellement si cette option est active, calculé avec clé de session K1.</p> <p><b>Il s'agit du scellement des données « FID » ou des données « FID+fichier ».</b></p>	

**Les champs 3, 4, 5, 6, 7, 8 et 9 ont les mêmes valeurs que dans le préfixe.**

## 7.11 Délimiteur de diffusion (format de base)

Ce délimiteur contient une partie variable, il ne suit pas exactement la règle de segmentation des délimiteurs. En effet, la numérotation des segments diffère car le nombre de segments peut être supérieur à 15. Les segments sont numérotés sur deux demi-octets. Le délimiteur de diffusion se place avant le délimiteur suffixe.

	CHAMPS	Type	Position de base	Longueur
0	Compteur longueur (bit de poids fort à 1)	B	1	2
1	Code enregistrement	B	3	3
2	Identifiant de diffusion (champ à usage réservé BdF)	B	6	1
3	Masque de diffusion (champ à usage réservé BdF)	B	7	24
4	Nombre de destinataires (noté N)	B	31	4
5	Sceaux de diffusion (Nx4 octets)	B	35	N x quatre
<b>TOTAL</b>				34 + Nx4

Champ 0	Compteur longueur
Sur deux octets, en base 256, indique la longueur de l'enregistrement qui suit.(le bit de poids fort est armé).	

Champ 1	Code enregistrement
1 <sup>er</sup> octet : #FO (hexadécimal) constante caractérisant le délimiteur de diffusion.	
2 <sup>ème</sup> octet et troisième octets :	
<ul style="list-style-type: none"> <li>• #11 et #11 en mode binaire</li> <li>• en format fixe <b>ou variable</b> : (voir 7.12.2 « Cas fixe ou variable avec compression »). <ul style="list-style-type: none"> <li>◇ octet 2: rang du segment (de #01 à #FF)</li> <li>◇ octet 3: nombre total de segments (de #01 à #FF)</li> </ul> </li> </ul>	

Champ 2	Identifiant de diffusion (champ à usage réservé BdF)
Lors de la diffusion d'un fichier vers plusieurs destinataires, la liste de diffusion est déterminée en utilisant un masque de recherche sur le premier identifiant ou le deuxième identifiant du fichier base de clé.	
<ul style="list-style-type: none"> <li>• #00 la comparaison est faite sur les premiers identifiants</li> <li>• #01 la comparaison est faite sur les deuxièmes identifiants</li> </ul>	

Champ 3	Masque de diffusion (champ à usage réservé BdF)
Lors d'une diffusion, l'agent ou l'application Banque de France indique sur quel critère un destinataire appartient à la liste. La liste est l'ensemble des couples identifiants dont le début de chaîne de caractère de l'identifiant utilisé correspond au masque.	
Le masque de comparaison (ex. "ZZZ4145FICP") peut être complété éventuellement par des espaces.	

Champ 4	Nombre de destinataires
Nombre (en caractères) de destinataires trouvés dans la base de clés de l'application émettrice	

Champ 5	Sceaux de diffusion
Cette zone contient autant de blocs de 4 octets que de destinataires. La taille de cette zone est de Nx4 octets (la valeur maximum de N dépend de la longueur des enregistrements mais ne doit pas dépasser 8000 en mode binaire).	
Chaque bloc est constitué des 4 premiers octets résultants du chiffrement DES(K1,3DES(KEK123destinataire,IV1 sceau du champ 10)).	

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	Date 02/01/2003
		Page 19 / 26

Le délimiteur est fragmenté suivant la structure du fichier (fixe ou variable) mais les segments sont numérotés différemment que pour les autres délimiteurs. Le bit de poids fort de la longueur de l'enregistrement ou des segments de cette zone est mis à 1.

## 7.12 Ajout des délimiteurs

Suite aux différentes opérations précédentes, le tampon sécurisé se retrouve de la forme :

```
□□EnregT1...□□EnregT2...□□...□□EnregTM...
```

□□ représente les deux octets du compteur de longueur de l'enregistrement de transport (lgT).

Il ne reste plus qu'à ajouter et adapter les délimiteurs pour compléter ce tampon.

### 7.12.1 CAS VARIABLE SANS COMPRESSION OU CAS BINAIRE

Les délimiteurs seront laissés dans leur format de base.

Pour le préfixe, les quatre premiers octets valent : #00 #A7 #11 #11.

Pour le suffixe, les quatre premiers octets valent : #80 #77 #11 #11.

### 7.12.2 CAS FIXE OU VARIABLE AVEC COMPRESSION

Le format de base du délimiteur est

```
□□Champ1Champ2...Dernierchampdudélimiteur
```

□□ représentant le champ 0 du délimiteur de base.

Champ1 contient constante caractérisant le délimiteur et une numérotation de segment

On élimine les champs 0 et 1 puis on complète le délimiteur par 32712 blancs (#20 si le fichier destiné au récepteur est codé en ASCII, #40 si le fichier est codé en EBCDIC).

```
Champ2...DernierchampdudélimiteurPaddingàblanc
```

Ensuite on découpe cette suite de champs à intervalle régulier en insérant 4 octets (5 octets pour le suffixe de diffusion) jusqu'au premier point d'insertion présent dans la zone de padding et on supprime la zone de padding superflue. Les octets insérés représentent : la longueur suivie d'un champ 1 contenant le numéro de segment.

```
■■⌚Seg1délim■■⌚Seg2délim...■■⌚SegNdélim...■■⌚DernierSegdélim■■Champ1padding
```

■■ compteur d'octet égal à lgT (bit de poids fort armé à 1 sauf pour le préfixe)

⌚ Champ 1 (2 ou 3 octets) avec le numéro de segment

Dans le cas du préfixe avec un chiffrement sans compression, le dernier octet du padding contient la longueur n du padding de chiffrement.

### 7.12.3 EXEMPLE DE SEGMENTATION ET DE PADDING

Pour un fichier dont les enregistrements sont tous de longueur 23 (*hors séquence de fin de ligne éventuelle*), la sécurisation en format fixe découpera le préfixe en 8 segments de 23 octets, chacun précédé d'un compteur de 2 octets (valeur #00#17 représentant la valeur décimale 23) :

1 <sup>er</sup> segment :	0017	0018	version délimiteur	type de codage	ident. émetteur (début)
2 <sup>ème</sup> segment :	0017	0028	identifiant émetteur (fin)	références complém. (début)	
3 <sup>ème</sup> segment :	0017	0038	références complémentaires (fin)	identifiant récepteur (début)	
4 <sup>ème</sup> segment :	0017	0048	ident. récepteur (fin)	type de fichier	nom du fichier (début)
5 <sup>ème</sup> segment :	0017	0058	nom du fichier (fin)	date et heure de création (début)	
6 <sup>ème</sup> segment :	0017	0068	date et heure de création (fin)	éléments de scellement (début)	
7 <sup>ème</sup> segment :	0017	0078	éléments de scellement (fin)	éléments de chiffrement (début)	
8 <sup>ème</sup> segment :	0017	0088	éléments de chiffrement (fin)	espaces de padding	

Le suffixe sera découpé en 6 segments de 23 octets :

1 <sup>er</sup> segment :	0017	FF16	version délimiteur	type de codage	ident. émetteur (début)
2 <sup>ème</sup> segment :	0017	FF26	identifiant émetteur (fin)	références complém. (début)	
3 <sup>ème</sup> segment :	0017	FF36	références complémentaires (fin)	identifiant récepteur (début)	
4 <sup>ème</sup> segment :	0017	FF46	ident. récepteur (fin)	type de fichier	nom du fichier (début)
5 <sup>ème</sup> segment :	0017	FF56	nom du fichier (fin)	date et heure de création (début)	
6 <sup>ème</sup> segment :	0017	FF66	date et heure de création (fin)	Sceau	

## 7.13 Format du fichier sécurisé

Le fichier sécurisé est donc le suivant

■■⊕Seg1prefixe..■■EnregT1..■■EnregT2..■■EnregTM..(■■⊕SegNDiffusion)..■■⊕DernierSegsuffixe
---

■■ représente les deux octets du compteur de longueur de l'enregistrement de transport (lgT).

⊕ Champ 1 du préfixe (2 octets) avec première séquence

⊕ Champ 1 du suffixe (2 octets) avec dernière séquence

s'il existe ⊕ Champ 1 de diffusion (3 octets) en séquence(ici le N<sup>ème</sup> segment)

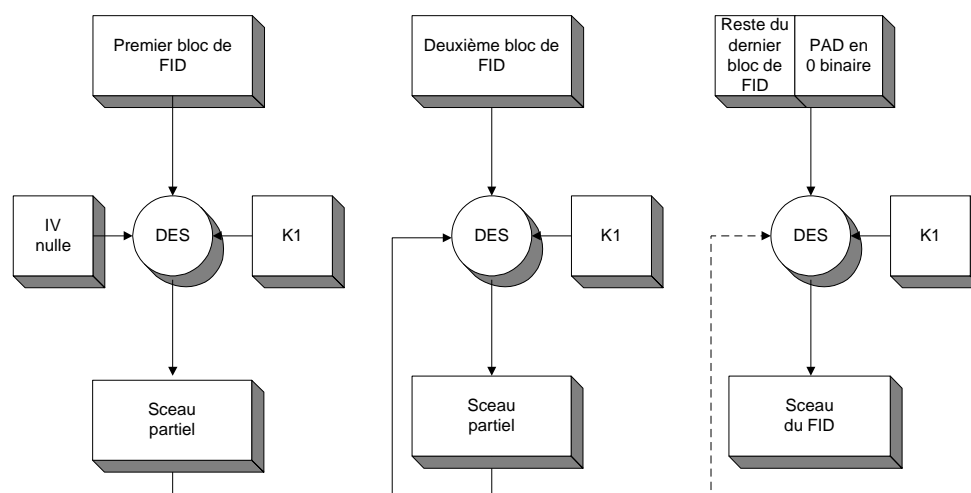
## 8 Mécanismes de sécurité

### 8.1 Authentification

Elle est réalisée au moyen du scellement du FID. Dans le cadre de ce scellement, les règles d'implémentation du DES sont les suivantes :

DES	en mode <b>CBC</b> (la sortie du bloc précédent sert de vecteur d'initialisation pour le bloc suivant)
clé	clé K1 de 64 bits tirée aléatoirement par le logiciel émetteur
IV	Vecteur d'Initialisation IV = 0 binaire d'une longueur de 64 bits
PAD	0 binaire en fin de FID pour obtenir une taille multiples de 8 octets
sceau	longueur de 64 bits

Le mécanisme garantit, du fait de l'horodatage, la non-reproductibilité du sceau en cas de retransmission du fichier.



**Figure 1 : mécanisme de l'authentification de l'origine du fichier**

Pour sceller le FID, SecurBdF V2 garde le même mécanisme.

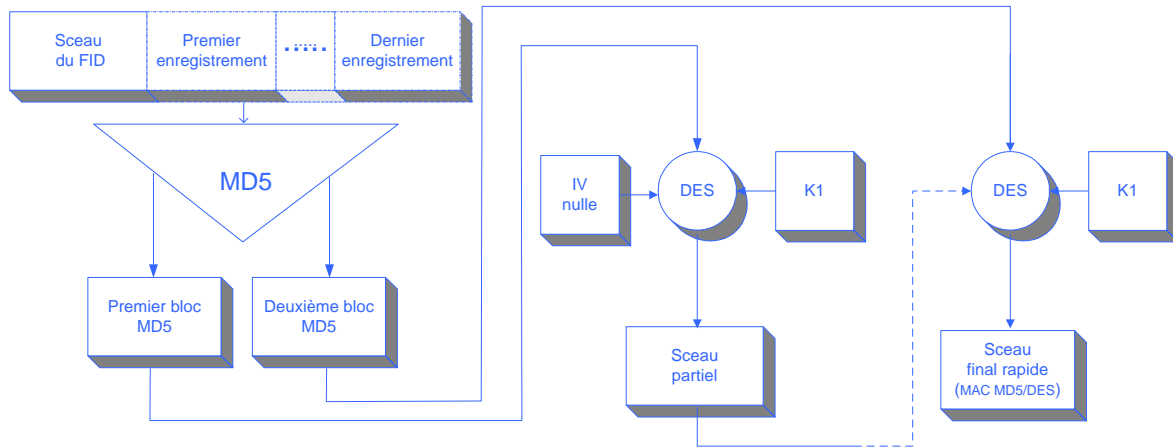
### 8.2 Intégrité des données

On calcule d'abord le MAC du FID comme pour une authentification d'origine normale puis on y concatène l'ensemble des enregistrements du fichier. Cette suite d'octets est condensée par la fonction MD5 qui fabrique un condensé de 16 octets. Enfin, on applique sur ce condensé un MAC DES avec un vecteur d'initialisation nul pour replier le résultat sur 8 octets.

Les règles d'implémentation du calcul MAC DES sont les suivantes :

DES	en mode <b>CBC</b>
clé	clé K1 de 64 bits utilisée pour l'authentification exposée ci-dessus
IV	Vecteur d'Initialisation IV = 0 binaire d'une longueur de 64 bits
sceau	longueur de 64 bits

Le schéma suivant illustre les mécanismes d'authentification et d'intégrité des données utilisées en mode V2 :



**Figure 2 : mécanisme de l'authentification et du scellement rapide en V2**

Dans le cas d'une utilisation du chiffrement et du scellement en simultané et sans l'utilisation de la compression, les enregistrements sont complétés comme pour un chiffrement (cf. 7.6 Adaptation du tampon (option chiffrement sans compression)).

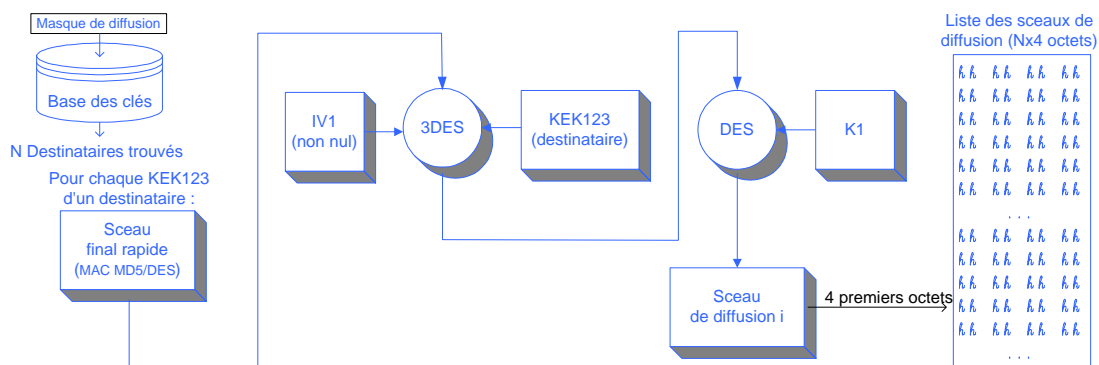
### 8.3 Intégrité des données en mode diffusion

La liste de diffusion peut être plus grande que la liste réelle des destinataires. Cette première est déterminée par comparaison d'un préfixe avec les identifiants situés dans la base de clé utilisée.

Pour chaque destinataire du fichier sécurisé unique :

DES	en mode EBC (sur un bloc équivalent à un mode CBC avec un vecteur nul)
Clé	clé K1 de 64 bits tirée aléatoirement par le logiciel émetteur (indiquée dans le préfixe du fichier sécurisé)
3DES	en mode CBC
Clé	clé KEK123 du destinataire
IV	le vecteur IV1 (non nul) indiqué dans le préfixe du fichier sécurisé (tiré aléatoirement par le logiciel émetteur)

Le schéma suivant résume le principe de diffusion :



**Figure 3 : mécanisme de diffusion**

Pour la réception, le destinataire effectue le calcul précédent avec la clé de sa base qui correspond au masque de diffusion (la dernière en cas de renouvellement). Puis il cherche les 4 octets calculés dans la table transmise dans le délimiteur de diffusion.

- S'il les trouve, le fichier est bien intègre et provient bien de la Banque de France.
- Dans le cas contraire, le fichier scellé ne provient pas de la Banque de France ou suite à un problème organisationnel l'établissement n'est pas dans la liste de diffusion du fichier.

On rappelle que le sceau « normal » doit être vérifié au préalable.

## 8.4 Confidentialité des données (hors compression)

Le chiffrement s'effectue par blocs de huit octets, enregistrement logique par enregistrement logique du tampon. Les règles d'implémentation du DES pour le chiffrement sont les suivantes :

DES ou 3DES	en mode CBC (choix DES ou 3DES suivant le niveau de confidentialité exigé par l'application)
Clé	clé K2 de 64 bits tirée aléatoirement par le logiciel émetteur
IV	Vecteur d'Initialisation IV2 de 64 bits (celui trouvé dans les éléments de sécurité du préfixe du fichier sécurisé) premier IV : tiré aléatoirement par le logiciel émetteur, mais non nul ensuite : réutilisation des 64 bits résultant du chiffrement de l'enregistrement "n" comme Vecteur d'Initialisation pour le chiffrement de l'enregistrement "n+1"

Le schéma suivant résume le principe du chiffrement.

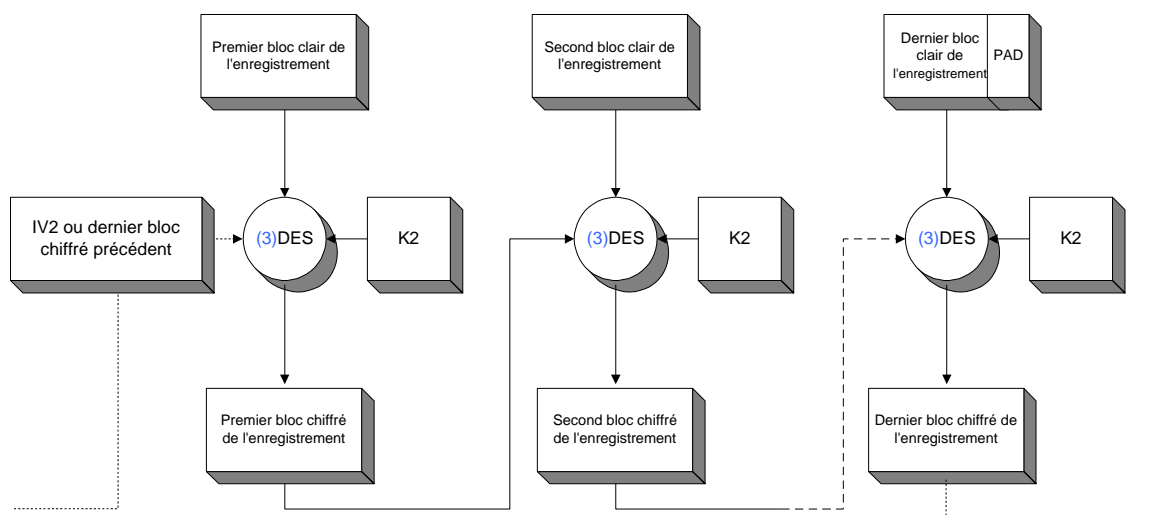


Figure 4 : mécanisme du chiffrement de chaque enregistrement

## 8.5 Confidentialité des données (avec compression)

Le chiffrement s'effectue par blocs de huit octets, sur la suite d'octet qui compose le tampon. On rappelle que la fin du tampon a été complétée pour que la taille du tampon soit un multiple de huit. Les règles d'implémentation du DES pour le chiffrement sont les suivantes :

DES ou 3DES	en mode CBC (choix DES ou 3DES suivant le niveau de confidentialité exigé par l'application)
Clé	clé K2 de 64 bits tirée aléatoirement par le logiciel émetteur
IV	Vecteur d'Initialisation IV2 de 64 bits (celui trouvé dans les éléments de sécurité du préfixe du fichier sécurisé) premier IV : tiré aléatoirement par le logiciel émetteur, mais non nul ensuite : réutilisation des 64 bits résultant du chiffrement du bloc précédent

Le schéma suivant résume le principe du chiffrement.

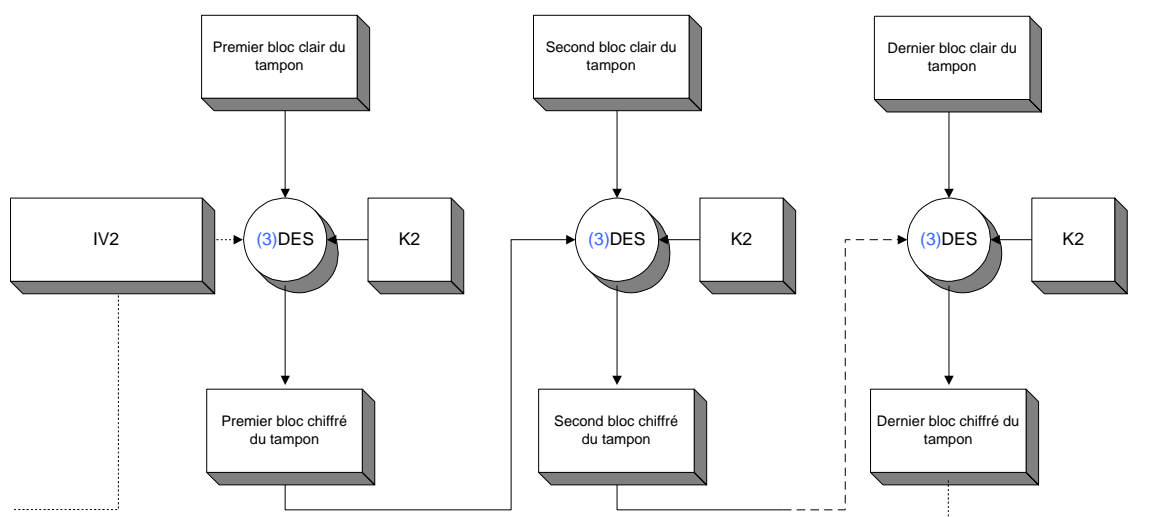


Figure 5 : mécanisme du chiffrement de chaque enregistrement

Protocole de sécurité de la Banque de France SecurBdF V2	Toute plate-forme	<b>Date</b> 02/01/2003
		<b>Page</b> 25 / 26

## A.1 ANNEXE A : Engagement de confidentialité

---

Le formulaire suivant est à retourner par les sociétés qui souhaiteraient implémenter le protocole de saisie de clés.

## ACTE D'ENGAGEMENT DE CONFIDENTIALITE

Nous, société \_\_\_\_\_ représentée par Monsieur (Madame) \_\_\_\_\_, en qualité de \_\_\_\_\_, certifions mettre en place tous les moyens techniques et humains nécessaires à la garantie de confidentialité des informations communiquées par la Banque de France dans le cadre du développement d'un module de saisie de clé compatible avec le protocole SecurBdF V2 de gestion de clés du RSI.

Nous nous engageons à ne pas copier, diffuser et divulguer à un tiers autre que les personnes dûment accréditées, dont les noms figureront explicitement dans la présente demande, et par quelque moyen que ce soit, les différentes informations contenues dans les documents que nous communiquerons à la Banque de France.

Dans l'hypothèse où nous déciderions de ne pas réaliser les développements, nous nous engageons à communiquer à la Banque de France la liste des personnes ayant eu accès aux informations fournies par celle-ci et à restituer à la Banque de France le document de spécifications du module de gestion de clés.

Fait pour valoir à \_\_\_\_\_

Le \_\_/\_\_/20\_\_

Signature précédée de la mention

« lu et approuvé »

P.J. Liste des personnes à accréditer

---