Ministère du budget, des comptes publics et de la fonction publique

Direction Générale de la Modernisation de l'Etat

Profils de Personnalisation des cartes IAS pour le support de l'administration électronique

V2.7

Middleware IAS

Profil de personnalisation des cartes IAS pour l'administration électronique

Référence	Date
MDWIAS_Profils de personnalisation des cartes IAS V2.7.doc	19/11/2007
Identification d'objet (OID)	**Racine OID et gestionnaire**
1.2.250.1.137.2.3.2.4.1	SDAE
Responsable	**Version**
DGME/SDAE	V2.7
Critère de diffusion	**Nombre de pages**
Public	135

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
21/12/06	2.0	Prise en compte des remarques des relecteurs	Gemalto J.M. Desjardins
22/06/07	2.1	Prise en compte remarques DGME. Modification lié à la modification de l'amendement 2 de la 7816-15.	Gemalto J.M. Desjardins
28/06/07	2.2	Ajout d'une annexe sur la taille des fichiers de l'application « GénériqueCrypto »	Gemalto J.M. Desjardins
03/07/2007	2.3	Ajout d'une annexe sur les règles d'encodage dchamp Longueur d'un Tag BER-TLV	Gemalto J.M. Desjardins
03/08/2007	2.4	Prise en compte remarques M. Schiavo (DGME/SDAE)	Gemalto J.M. Desjardins
29/08/2007	2.5	Ajout de l'extended path pour pointer sur les fichiers EF_ID et EF_AD (§ 6.3.6 -)	Gemalto J.M. Desjardins
28/09/2007	2.6	Ajout d'une recommandation pour la gestion du PIN Global (§ 4.1.2)	Gemalto A.Lotigier
19/11/2007	2.7	Ajout de recommandations pour le déblocage du PIN Global (§ 4), mise a jour correspondante des SE et des fichiers EF_AOD.	Gemalto A.Lotigier

Sommaire

Table des figures

Tables des tableaux

1 - INTRODUCTION

Ce document décrit des implémentations de référence ou cibles des applications cryptographiques envisagées pour les cartes utilisée dans le cadre de l'administration électronique (Vitale 2, CNIe, CVQ, cartes Agents et autres).

Ces applications visent à permettre l'acceptation de la carte par des logiciels s'appuyant sur les interfaces standards PKCS#11 ou MS CAPI ou par des logiciels s'appuyant sur les interfaces spécifiques : IAS API. Ces trois modules d'interface font partie du pilote carte IAS ou MiddleWare IAS.

Ces trois modules permettent d'accèder aux fonctions cryptographiques, y compris aux fonctions de mise à jour de clés et de certificats.

Trois applications cryptographiques sont décrites dans ce document. Ces applications **peuvent** coexister **ou non** au sein d'une même carte. De plus les applications sont décrites dans leur version maximale respective. Ainsi en fonction des besoins réels, certains objets peuvent ne pas être présents. L'annexe B présente les objets obligatoires, optionnels et conditionnels pour chacune des applications. Certains paramètres pourraient aussi être adaptés, c'est le cas notamment de l'emplacement du fichier Identité du porteur. Les paramètres modifiables sont :

- L'emplacement des fichiers identité, adresse et numéro de série.
- Les attributs d'accès à ces fichiers. Notamment dans cette version du document, le numéro de série est libre en lecture, il est possible d'envisager d'autres combinaisons. Cependant, les conditions d'accès les plus restrictives devront être adoptées par l'ensemble des propriétaires des applications d'une carte. Le numéro de série est une information identifiant une carte et une seule.

Les trois applications décrites ci-après sont :

- **L'application Adèle -Administrateur 1 :** Cette application est destinée à supporter les fonctions cryptographiques classiques (Authentification, Signature et Déchiffrement) **conformément aux exigences PRISV2**. Cette application supporte notamment la signature qualifiée. L'application Adèle est supportée par PKCS#11 et MS CAPI uniquement pour les fonctions d'exploitation des clés et des certificats. Les fonctions de mises à jour sont supportées par l'API IAS spécifique du logiciel d'interface : middleware IAS.

  Dans cette spécification, l'application Adèle contient :
  - une bi-clé d'authentification et son certificat associé
  - une bi-clé de signature et son certificat associé
  - une bi-clé de confidentialité et son certificat associé

D'autres bi-clés et certificats peuvent être présents mais ils doivent avoir les mêmes contrôles d'accès que les 3 couples bi-clés/certificats mentionnés ci-dessus et avoir été référencé dans les fichiers PKCS#15 décrits dans cette spécification.

La bi-clé de signature et son certificat associé peuvent être qualifiés. On parle alors aussi de bi-clé *** et de certificat ***. Dans ce cas, la présence d'un PIN de signature PIN_Sign et des objets nécessaires à son exploitation (déblocage) sont obligatoires. L'application Adèle fait aussi référence à une zone Identité hébergée par l'émetteur. Les besoins en terme de sécurité (contrôle d'accès) sont décrits dans ce document.

Cette définition de l'application Adèle est le résultat d'un groupe de travail inter ministériel.

- **L'application Adèle –Administrateur 2:** Cette application est destinée à supporter les fonctions cryptographiques classiques (Authentification, Signature et Déchiffrement) dans un contexte analogue à celui de l'application Adèle. Plus précisément, la mise à jour des objets de l'application se fait sous contrôle d'un administrateur (en « secure-messaging ») pouvant être différent de celui gérant l'application Adèle. Dans cette spécification l'application Adèle Administrateur 2 contient :

  - une bi-clé d'authentification et son certificat associé
  - une bi-clé de signature et son certificat associé
  - une bi-clé de confidentialité et son certificat associé

L'application Adèle-Administrateur 2 est identique à l'application Adèle-Administrateur 1. Cependant, elle ne supporte pas la signature qualifiée car une seule application supportant la signature qualifiée peut être présente dans la carte. L'administration proposant le service de signature qualifiée dans la carte doit utiliser l'application Adèle-Administrateur 1 protégée avec son jeu de « clés autorités administratives ».

- **L'application Adèle « générique » :** Cette application est destinée à supporter les fonctions cryptographiques classiques (Authentification, Signature et Déchiffrement) **dans le contexte MSCAPI/PKCS#11 y compris en mise à jour**. Aussi les conditions d'accès aux objets sont réduites à libre ou protégé par PIN global. Toute application existante s'appuyant sur ces couches logicielles doit pouvoir sans aucune modification gérer la carte comme outil cryptographique. Dans cette spécification, l'application Adèle Générique contient :

  - une bi-clé d'authentification et son certificat associé
  - une bi-clé de signature et son certificat associé
  - une bi-clé de confidentialité et son certificat associé

D'autres bi-clés et certificats peuvent être présents mais ils doivent avoir les mêmes contrôles d'accès que les 3 couples bi-clés/certificats mentionnés ci-dessus et avoir été référencés dans les fichiers PKCS#15 décrits dans cette spécification.

L'émetteur de cartes d'une autorité administrative devra adapter la présente spécification à ses besoins et compléter la personnalisation de la carte par sa partie propre appelée application Emetteur.

2 - TERMINOLOGIE & REFERENCES

2.1 - Références

Notation	Description
[IAS]	Plateforme Commune pour l'eAdministration – Spécification technique Version 1.01 Premium
[PRISV2]	Disponible sur www.synergies.modernisation.gouv.fr
[7816-15]	ISO/IEC 7816-5 standard 2004-01-15
[IAS-REF]	Programme de référencement des produits IAS et tests de conformité disponible sur www.synergies.modernisation.gouv.fr

2.2 - Terminologie

Abbréviations utilisées dans ce document:

Notation	Description
SMI PSCe	"Secure Messaging" en intégrité uniquement se référant au jeu de clés d'administration de l'application Adèle Administrateur 1 ou 2
SMIC PSCe	"Secure Messaging" en intégrité et confidentialité se référant au jeu de clés d'administration de l'application Adèle Administrateur 1 ou 2
SMI AA	"Secure Messaging" en intégrité uniquement se référant au jeu de clés d'utilisation des Autorités Administratives.
PIN_Sign	Code d'authentification du Porteur dédié à la Signature électronique. Ce code d'authentification est propre à l'application Adèle. Ce code n'est utilisé que dans le cas de signature ***
PIN_Global	Code d'authentification du Porteur de la carte. Ce code est valide pour l'ensemble de la carte.
PUK_Global	PIN de déblocage du PIN global
PUK_Sign	Code de déblocage du code de signature
PSCe_KeySet	Jeu de clés administratives de l'application.
AA_KeySet	Jeu de clés de gestion du « Secure Messaging » dédié aux Autorités Administratives
Sign_KeySet	Jeu de clés de gestion du « Secure Messaging » dédié à la signature ***.

2.3 - Notation

Notation	Description
“ABCD “	Représente la chaîne de caractères ASCII “ABCD”.
0x313233 or 0x 31 32 33	Représente le nombre Hexadécimal 313233 soit 3 224 115 en décimal Dans le document, toutes les valeurs sont fournies en hexadécimal excepté lorsque explicitement notifié.

3 - Caractéristiques des applications cryptographiques supportées par le middleware IAS

Ce chapitre présente les architectures possibles pour des applications cryptographiques supportées par le middleware IAS. Toute application cryptographique conforme à l'une de ces architectures et dont l'application CIA associée possède un AID dont les 7 premiers octets sont '0xE8 28 BD 08 0F D2 50' est supportée par le middleware.

Ces applications peuvent être activées depuis plusieurs supports :

- Carte d'identité nationale CNIE,
- Carte Vitale 2,
- Carte Agent,
- Ou toute autre carte basée sur le socle commun IAS

Les applications présentées dans ce document sont au nombre de trois :

- L'application Adèle ou Adèle Administrateur 1. Cette application est destinée à supporter les besoins de l'administration, plus particulièrement cette application supporte la signature qualifiée (profil ***).
- L'application Adèle Générique. Cette application est destinée aux cartes agents en complément de l'application Adèle. Cette application supporte notamment le « SmarCard Logon » et est interfaçable par toute application utilisant les API MS CAPI et PKCS#11.
- L'application Adèle Administrateur 2. Cette application est une application identique à l'application Adèle mais gérée par un autre administrateur. Cependant l'application Adèle Administrateur 2 ne supporte pas la signature qualifiée. L'application Adèle doit être utilisée pour la signature qualifiée. En effet le support de la signature qualifiée impose un PIN de signature, et il n'est pas envisagé que le porteur de carte utilise 2 PINs de signature qualifiée en plus du PIN Global.

La présente spécification décrit une application Adèle ou Adèle – Administrateur 1 dans sa version maximale.

En fonction des besoins et du support l'application Adèle pourra cependant posséder des caractéristiques différentes. C'est le cas des données d'identification du porteur. En effet celles-ci pourront être gérées de manière différente en fonction du type de carte. De plus, l'application Adèle peut varier, en fonction des besoins du porteur et/ou de l'administration. Une des variantes est le niveau de sécurité associé à la signature. On parle de niveau *, ** pour une signature électronique « standard » et de niveau *** pour une signature dite qualifiée. Le document [PRISv2] décrit les exigences des différents niveaux de sécurité. Ces critères ne se limitent pas aux clés de signature mais à toute clé. Aussi dans ce document, un profil est établi en fonction du niveau de sécurité auquel le porteur ou l'administration veut accéder, sachant que le niveau * ou ** partage le même profil technique, seules les tailles des secrets diffèrent.
Le profil de la carte agent est un profil intégrant à la fois une application Adèle telle que décrite dans ce document ainsi qu'une application générique Adèle Générique afin de supporter entre autre le smartcard logon ainsi que le chiffrement, la signature de mèls.

L'application Adèle ou Adèle – Administrateur 1 se compose de deux sous répertoires :

- Le répertoire Adèle : Ce répertoire contient l'ensemble des éléments cryptographiques nécessaires à l'exploitation des services offert par l'application y compris les éléments nécessaires à la maintenance de l'application.
- Le sous répertoire CIA Adèle : Ce répertoire contient les deux fichiers EF.CIAInfo et EF.OD décrits dans la norme ISO 7816-15.

Les applications Adèle Générique et Adèle Administrateur 2 sont gérées depuis le répertoire CIA correspondant.

3.1 - L'application Adèle Administrateur 1 - Profil * ou **

La figure suivante montre l'architecture fichier de l'application Adèle au sein d'une carte pour une application avec un niveau * ou **.

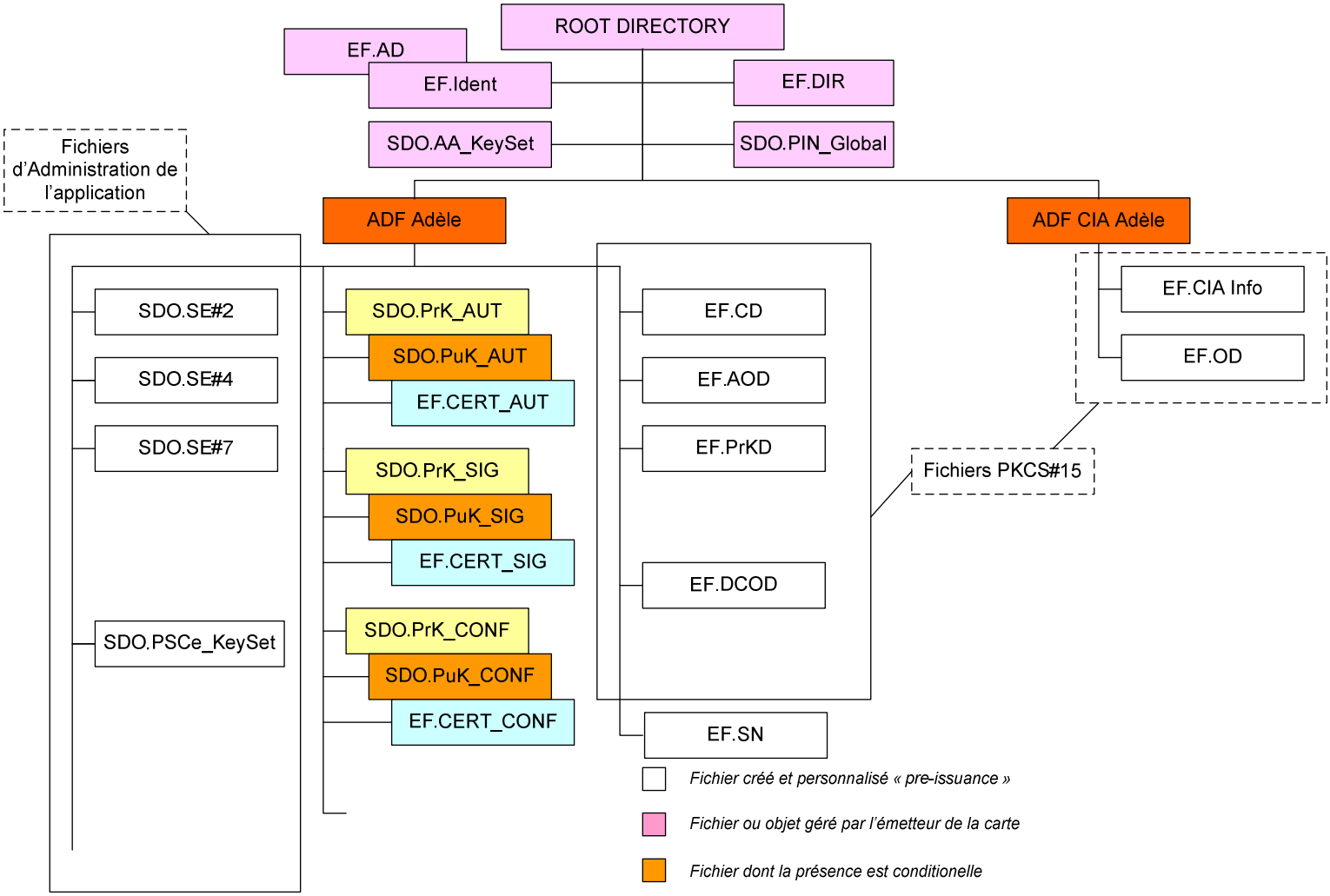

Figure 3-1 : Profil * ou ** : Architecture de fichiers

Les SE #2 et #4 sont dédiés à l'administration de l'application. Le SE#7 est dédié à l'exploitation des fonctions cryptographiques (i.e. à la gestion des protections des fonctions cryptographiques).
Les clés privées peuvent être soient générées par la carte soit générées par une Autorité de Certification et inscrites dans la carte sous contrôle du PSCe. Dans le cas où les clés privées doivent être générées par la carte, les SDOs « clé publique » correspondants doivent avoir été créés.

3.2 - L'application Adèle Administrateur 1 - Profil ***

La figure suivante montre l'architecture fichier de l'application Adèle au sein d'une carte pour une application avec un niveau ***.

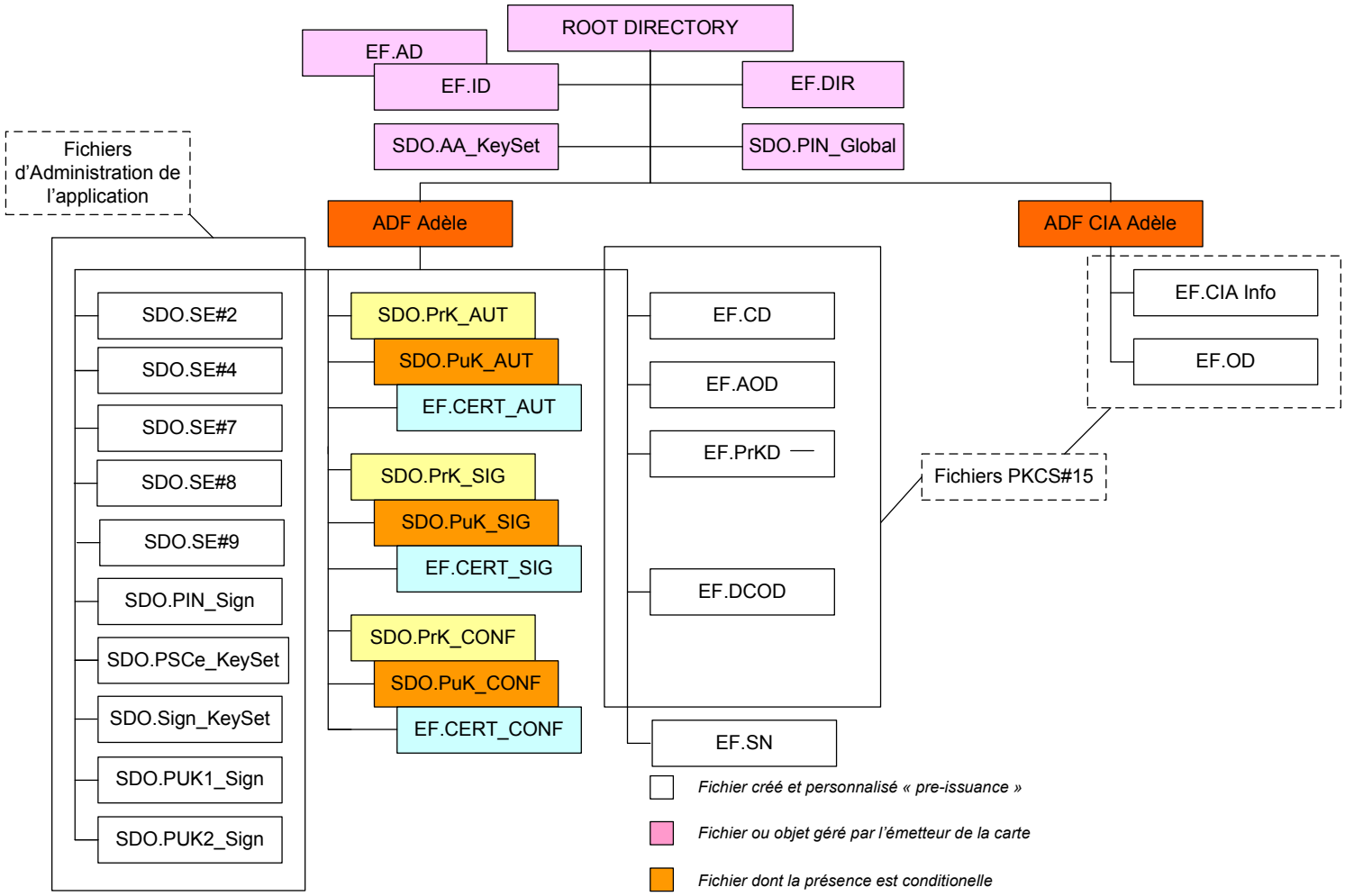

Figure 3-2 : Profil * : Architecture de fichiers**

Les SE #2 et #4 sont dédiés à l'administration de l'application. Le SE#7 est dédié à l'exploitation des fonctions cryptographiques ou signature. Le SE #8 est dédié à l'exploitation de la signature.
Les clés peuvent être générées par la carte, les fichiers de clé publique sont alors nécessaires.

Les cartes (typiquement les cartes Agent) peuvent aussi supporter une autre application, appelée Application Adèle Générique. Cette application a été élaborée de manière à pouvoir être interfacée en écriture par une couche PKCS#11.

3.3 - L'application Adèle Générique

Cette application est une application « CIA » contenant l'ensemble des éléments. L'EF.DCOD peut être présent. Néanmoins il n'est pas utile de pointer des éléments comme le numéro de série de la carte ou le fichier identité qui sont déjà pointé par d'autres applications CIA.

L'ensemble des fichiers et des objets sont créés durant la personnalisation de la carte. Néanmoins nombre de ces fichiers peuvent ne pas être initialisés en phase de personnalisation de la carte.

La figure suivante illustre l'architecture fichier/Objet de cette application.

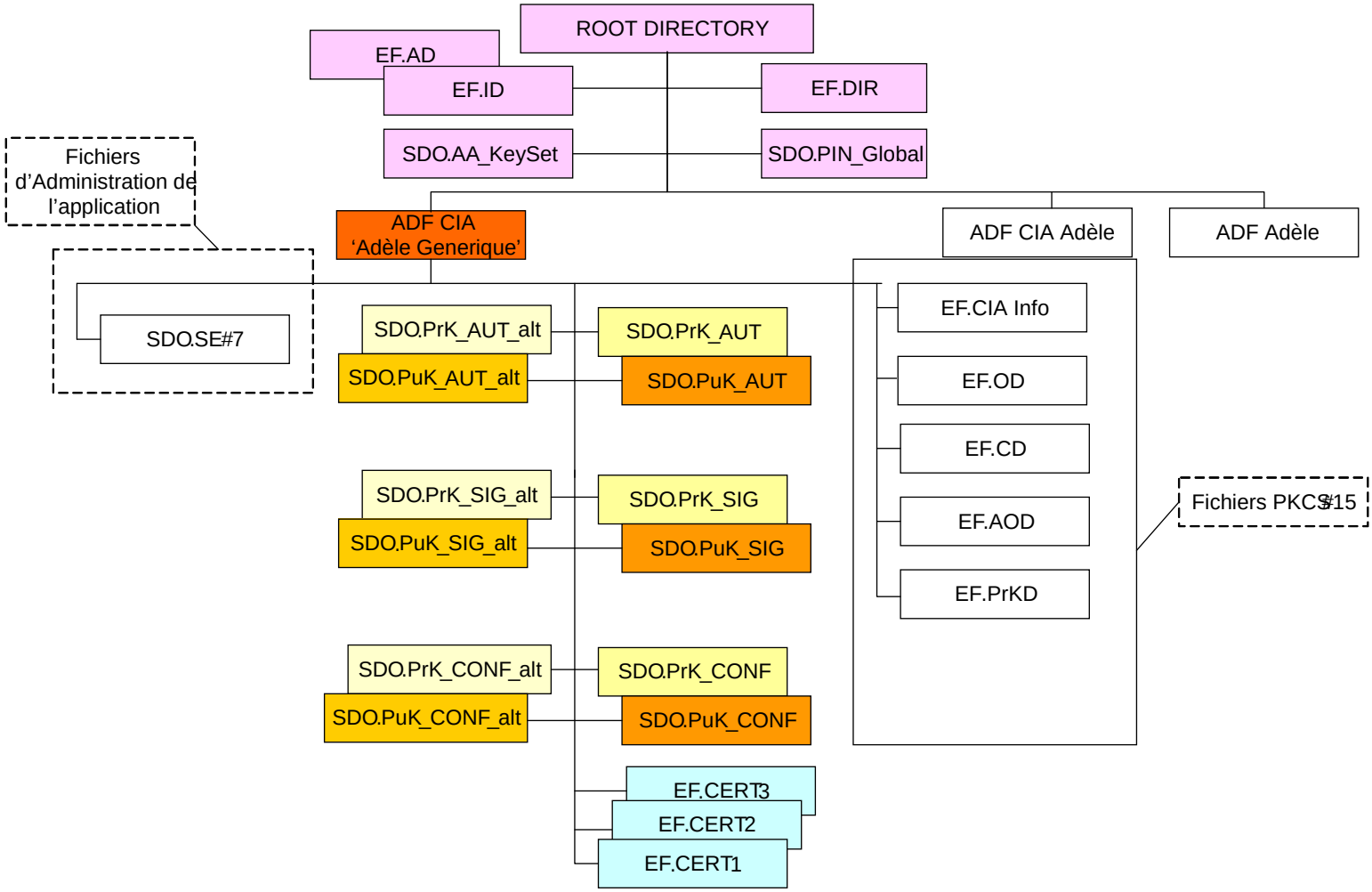

Figure 3-3 : Architecture Fichier de l'application Adèle Générique

3.4 - L'application Adèle Administrateur 2

Cette application est quasi identique à l'application Adèle. Cependant cette application ne supporte pas de signature et certificats qualifiés.

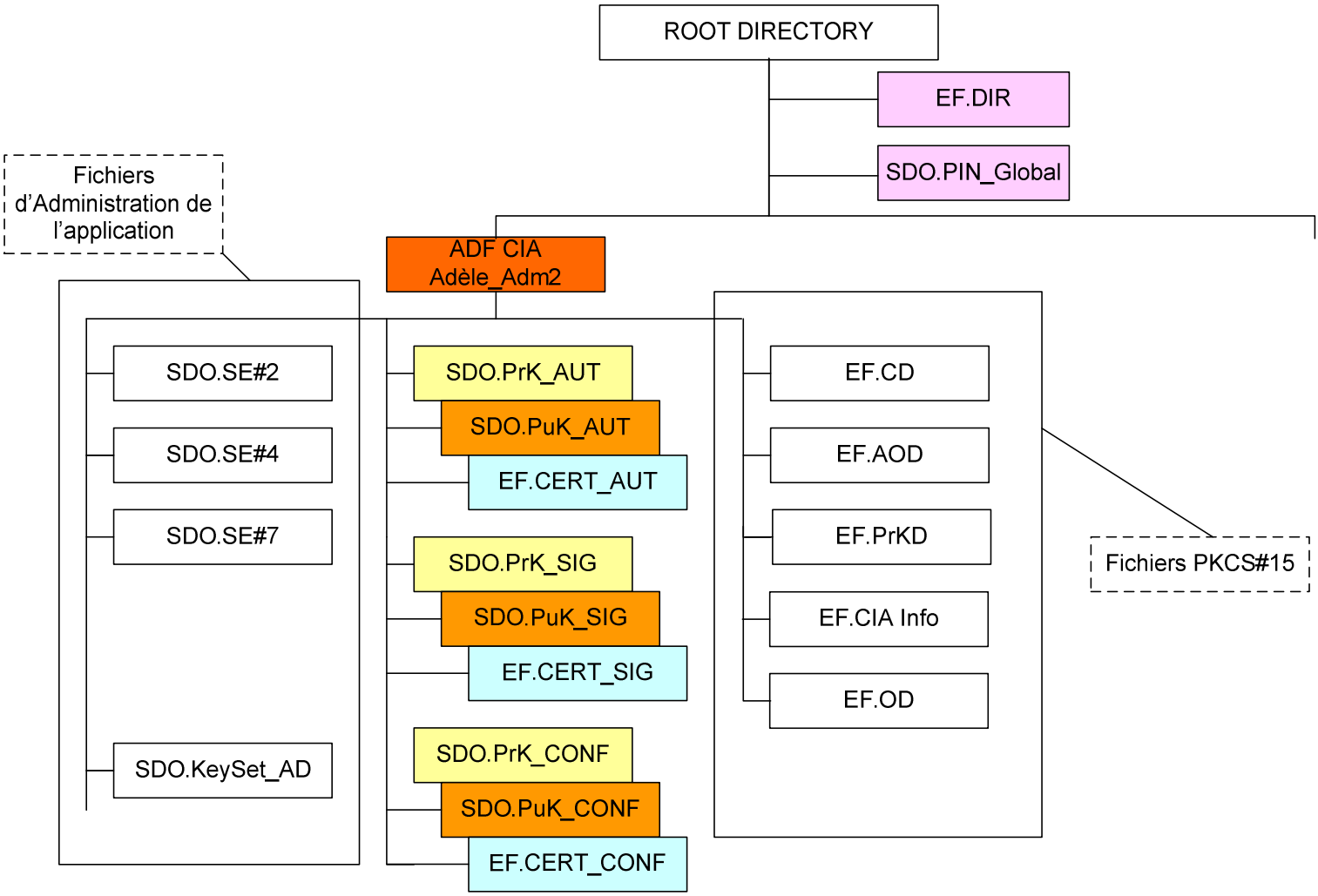

Figure 3-4 : Architecture fichier de l'application Adèle Administrateur 2

4 - Root Directory

Cette application est sous le contrôle exclusif de l'émetteur de la carte.

Pour des besoins d'interopérabilité, les objets suivants doivent être présent au niveau du ROOT directory :

- **Le fichier EF-DIR contenant la liste des applications supportées par la carte.**
- **Un code appelé PIN Global destiné à l'authentification du porteur.**
- **Des fichiers contenant des données d'identification du porteur.**

La gestion du code Pin (fourniture, déblocage, changement) est définie par l'émetteur. Il est utilisé par l'application Adèle pour protéger les authentifications « Clients/Serveurs », le chiffrement, la signature dans le cas de profil * ou **.

4.1 - Fichiers ou Objets

4.1.1 - 2F00 - EF-DIR

Ce fichier contient les différentes applications présentes dans la carte.

.

Le fichier EF-DIR doit contenir un descripteur par application. Ici ne sont décrits que les descripteurs des applications présentes dans la carte :

- Adèle et CIA Adèle
- Adèle Générique (application de type CIA)
- Adèle administrateur 2 (application de type CIA).

En-tête du fichier:

Tag	L	Description			
62	LL	File Control Parameter (FCP)			
		Tag	**L**	**Description**	**Valeur**
		80	02	File size	*A définir*
		82	01	File descriptor	0x01 (EF transparent)
		83	02	File Identifier	0x2F00
		88	01	Short File identifier	0X1E
		A5	xx	Proprietary Information	*A définir – Optionnel*
		85	xx	Proprietary Information	*A définir – Optionnel*
		8A	01	Life cycle State	*A définir*
		8C	xx	*Compact Security Attributs*	*A définir*

En fonction des caractéristiques de la carte, les attributs de sécurité du fichier peuvent être modifiés. La lecture du fichier **doit être libre** ; sa mise à jour doit être protégée en accord avec les possibilités de créer, effacer des applications. Dans le cas où, créer ou effacer des applications sont des opérations interdite, la mise à jour de l'EF-DIR doit cependant être autorisée.

Descripteur de l'application CIA Adèle :

Tag	L	Description			Valeur
61	28	*Application template*			
		Tag	**L**	**Description**	**Valeur**
		4F	0F	AID associé au CIA Adèle	0xE8 28 BD 08 0F D2 50 00 00 04 01 01
		50	06	Application Label " Adèle"	0x41 64 C3 A8 6C 65 (« Adèle » UTF8 encoded)
		Tag	**L**	**Description**	**Valeur**
		73	0E	CIODDO Proprietary object. Voir ci-dessous	0x4F 0C D2 50 00 00 04 41 64 E8 6C 65 01 01

Descripteur de l'application Adèle :

Tag	L	Description				Valeur
61	Var	*Application template*				
		Tag	**L**	**Description**		**Valeur**
		4F	0C	AID application Adèle		0xD2 50 00 00 04 41 64 E8 6C 65 01 01
		50	06	Application Label " Adèle"		0x41 64 C3 A8 6C 65 (« Adèle » UTF8 encoded)
		73	var	*Données discrétionnaires*		
			Tag	**L**	**Description**	**Valeur**
			06	Var	OID. Identification du niveau de conformité à la spécification IAS. Défini par la DGME/SDAE.	
			42	05	IIN	0x8025000002

L'AID de l'application Adèle se compose :

- d'un RID (Registered Identifier sur 5 octets) 0xD2 50 00 00 04
- d'un PIX (Proprietary Identifier -11octets au max).

Pour l'application Adèle, le PIX est composé comme suit :

- De 5 octets : 0x 41 64 E8 6C 65 (codage ASCII de 'Adèle').

- Suivi de deux octets ayant la signification suivante :
  - L'octet de poids fort spécifie le type de l'application Adèle :
    01 pour Adèle -Administrateur 1

  - L'octet de poids faible précise la version de spécification de personnalisation de référence : 01 désigne cette spécification. Il pourrait être en effet nécessaire pour certains logiciels applicatifs de savoir où chercher certains fichiers (fichiers non couverts par la norme 7816-15 par exemple).

Pour les applications CIA, les AIDs sont construits de la manière suivante :

- d'un RID (Registered Identifier sur 5 octets) normalisé : 0xE8 28 BD 08 0F
- d'un PIX (Proprietary Identifier -11octets au max). constitué comme suit :
  - De 5 octets rappelant le RID de l'application Adèle : 0x0xD2 50 00 00 04
  - Suivi de deux octets ayant la signification suivante :
    - L'octet de poids fort spécifie le type de l'application Adèle :
      01 pour Adèle -Administrateur 1
      02 pour Adèle -Administrateur 2
      03 pour Adèle Générique
    - L'octet de poids faible précise la version de spécification de personnalisation de référence : 01 désigne cette spécification. Il pourrait être en effet nécessaire pour certains logiciels applicatifs de savoir où chercher certains fichiers (fichiers non couverts par la norme 7816-15 par exemple).

Le template de l'application CIA Adèle est composé comme suit :

- De l'AID de l'application (Tag '4F')
- Du « label » associé (Tag '50') à cette application. Le label est : « Adèle ». Le label de l'application CIA est identique à celui de l'application associé.
- D'un template contenant :
  - Le CIODDO associé à chaque application CIA (sous le tag '73' et non 'A5' comme indiqué dans la spécification IAS – Le tag 'A5' est en effet non décrit dans les normes 7816 comme étant un tag possible dans ce contexte).

CIODDO ::= SEQUENCE

{

providerID OPTIONAL,	-- Elément optionnel, identifie le « fournisseur » de l'application CIA
odfPath OPTIONAL,	-- Elément optionnel décrit le chemin d'accès au fichier EF_OD quand celui –ci ne se trouve pas dans le répertoire CIA. Dans le cas présent ce champ n'est pas renseigné.
ciaInfoPath OPTIONAL,	-- Elément optionnel décrit le chemin d'accès au fichier EF_CIAinfo quand celui –ci ne se trouve pas dans le répertoire CIA Dans le cas présent ce champ n'est pas renseigné.
aid '0xD2 50 00 00 04 41 64 E8 6C 65 01 01',	

}

Seul l'objet **aid** est à renseigner. Ce qui donne :
0x4F 0C D2 50 00 00 04 41 64 E8 6C 65 01 01

Le tag CIODDO SEQUENCE ('30') est remplacé par le tag '73' voir [ISO 7816-4] [ISO 7816-15]

Le template de l'application Adèle est composé comme suit :

- De l'AID de l'application (Tag '4F')
- Du « label » associé (Tag '50') à cette application. Le label est : « Adèle ».
- D'un template contenant :
  - Un OID permettant d'identifier la conformité de la carte aux spécifications IAS. Cet OID permettra aussi de référencer la version de spécification. Cet OID est déterminé par le DGME/SDAE. Les valeurs doivent être prises conformément au document [IAS-REF]
  - Un IIN permettant d'identifier l'entité émettrice de la carte.

Descripteur de l'application CIA Adèle Générique :

<table>
<tr><th>Tag</th><th>L</th><th colspan="3">Description</th><th>Valeur</th></tr>
<tr><td>61</td><td>28</td><td colspan="4">Application template</td></tr>
<tr><td colspan="2" rowspan="4"></td><td>Tag</td><td>L</td><td>Description</td><td>Valeur</td></tr>
<tr><td>4F</td><td>0F</td><td>AID associé au CIA Adèle Générique</td><td>0xE8 28 BD 08 0F D2 50 00 00 04 03 01</td></tr>
<tr><td>50</td><td>12</td><td>Application Label “ Adèle Générique ”</td><td>0x41 64 C3 A8 6C 65 20 47 C3 A9 72 C3 A9 72 69 71 75 65 (« Adèle Générique» UTF8 encoded)</td></tr>
<tr><td>Tag</td><td>L</td><td>Description</td><td>Valeur</td></tr>
<tr><td colspan="2"></td><td>73</td><td>0E</td><td>CIODDO Proprietary object. Voir ci-dessous</td><td>0x4F 0C E8 28 BD 08 0F D2 50 00 00 04 03 01</td></tr>
</table>

CIODDO ::= SEQUENCE

{

providerID OPTIONAL, -- Elément optionnel, identifie le « fournisseur » de l'application CIA

odfPath OPTIONAL, -- Element optionnel décrit le chemin d'accès au fichier EF_OD quand celui –ci ne se trouve pas dans le répertoire CIA. Dans le cas présent ce champ n'est pas renseigné.

ciaInfoPath OPTIONAL, -- Element optionnel décrit le chemin d'accès au fichier EF_CIAinfo quand celui –ci ne se trouve pas dans le répertoire CIA Dans le cas présent ce champ n'est pas renseigné.

aid 'AID ',de l'application CIA Adèle Générique

}

Seul l'objet **aid** est à renseigner. Il est renseigné avec l'AID de l'application CIA Adèle Générique. Ce qui donne :
Ox4F 0C E8 28 BD 08 0F D2 50 00 00 04 03 01

Descripteur de l'application CIA Adèle -Administrateur 2

Tag	L	Description			Valeur
61	48	*Application template*			
		Tag	**L**	**Description**	
		4F	0F	AID associé au CIA Adèle -Administrateur 2	0x E8 28 BD 08 0F D2 50 00 00 04 02 01
		50	25	Application Label "Adèle -Administrateur 2"	0x41 64 C3 A8 6C 65 20 2D 41 64 6D 69 6E 69 73 74 72 61 74 65 75 72 20 32 (« Adèle - Administrateur 2» UTF8 encoded)
		Tag	**L**	**Description**	
		73	0E	CIODDO Proprietary object. Voir ci-dessous	0x4F 0C E8 28 BD 08 0F D2 50 00 00 04 02 01

Le template de l'application CIA Adèle Administrateur 2 est composé comme suit :

- De l'AID de l'application (Tag '4F')
- Du « label » associé (Tag '50') à cette application. Le label est : « Adèle -Administrateur 2».
- D'un template contenant :
  - Le CIODDO associé à chaque application CIA.

CIODDO ::= SEQUENCE
{
providerID OPTIONAL, -- Elément optionnel, identifie le « fournisseur » de l'application CIA
odfPath OPTIONAL, -- Elément optionnel décrit le chemin d'accès au fichier EF_OD quand celui –ci ne se trouve pas dans le répertoire CIA. Dans le cas présent ce champ n'est pas renseigné.
ciaInfoPath OPTIONAL, -- Elément optionnel décrit le chemin d'accès au fichier EF_CIAinfo quand celui –ci ne se trouve pas dans le répertoire CIA Dans le cas présent ce champ n'est pas renseigné.
aid,
}

Seul l'objet **aid** est à renseigner. Ce qui donne :
0x4F 0C E8 28 BD 08 0F D2 50 00 00 04 02 01
Le tag CIODDO SEQUENCE ('30') est remplacé par le tag '73' voir [ISO 7816-4] [ISO 7816615]

Le template de l'application Adèle Administrateur 2 est composé comme suit :

- De l'AID de l'application (Tag '4F')
- Du « label » associé (Tag '50') à cette application. Le label est : « A compléter ».
- D'un template contenant :
  - Un OID permettant d'identifier la conformité de la carte aux spécifications IAS. Cet OID permettra aussi de référencer la version de spécification. Cet OID est déterminé par le DGME/SDAE. Les valeurs doivent être prises conformément au document [IAS-REF].

4.1.2 - Gestion du PIN Global

Le PIN Global se trouve au niveau du « root » et est géré par l'émetteur de la carte. Plus précisément, le PIN est généré, distribué, mis à jour et débloqué selon les règles édictées par l'émetteur.

Ce paragraphe présente des recommandations pour l'implémentation du PIN Global et d'un PIN de déblocage associé.

Note : la fonction de déblocage du PIN Global est supportée par l'API IAS spécifique du logiciel d'interface (middleware IAS).

Caractéristique de l'Objet PIN Global :

Tag	L	Description	Valeur
FF8101	30	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	17	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 06
84	0A	Nom de l'objet de sécurité	"PIN Global"
8C	05	Attribut de sécurité "compact"	0xF1 17 00 16 00

CHANGE REFERENCE DATA	PIN Global
VERIFY	Libre
RESET RETRY COUNTER	PUK Global
RFU	Interdit
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
9A	01	Nombre maximum d'essais autorisés	0x03
9B	01	Compteur d'essais	0x03
7F41	0E	*Valeur du PIN*	

Tag	L	Description	Valeur
80	01	Taille maximum	0x04
81	01	Taille minimum	0x04
82	06	Valeur du PIN	0x31323334

La vérification du PIN de déblocage peut être soit libre, soit protégée en secure messaging avec un jeu de clés d'administration, selon la politique de sécurité de l'émetteur.

Note : les descriptions ci-dessous de l'objet PIN de déblocage du PIN Global sont données à titre d'exemple. Notamment les conditions d'accès de l'objet PIN de déblocage peuvent être modifiées en fonction de la politique de sécurité définie par l'émetteur.

Exemple d'objet PIN de déblocage du PIN Global (PUK Global), avec vérification libre:

Tag	L	Description				Valeur	
FF8102	33	*Référence de l'objet*					
		Tag	**L**	**Description**			
		E2	1B	*DOCP*			
			Tag	**L**	**Description**		
			80	02	Longueur du DOUP	0x00 06	
			84	10	Nom de l'objet de sécurité	'PUK Global'	
			8C	04	Attribut de sécurité « compact"	0xE1 16 00 00	
						CHANGE REFERENCE DATA	PUK Global
						VERIFY	Libre
						RESET RETRY COUNTER	Interdit
						RFU	Interdit
						RFU	Interdit
						PUT DATA	Interdit
						GET DATA	Libre
		9A	01	Nombre maximum d'essais autorisés		03	
		9B	01	Compteur d'essais restant		03	
		7F41	E	*Valeur du PIN*			
			Tag	**L**	**Description**		
			80	01	Taille maximum	06	
			81	01	Taille minimum	06	
			82	06	Valeur du PUK	*Typiquement dérivée d'une clé mère*	

Exemple d'objet PIN de déblocage du PIN Global (PUK Global), avec vérification en secure messaging:

Tag	L	Description				Valeur	
FF8102	33	*Référence de l'objet*					
		Tag	**L**	**Description**			
		E2	1B	*DOCP*			
			Tag	**L**	**Description**		
			80	02	Longueur du DOUP	0x00 06	
			84	10	Nom de l'objet de sécurité	'PUK Global'	
			8C	03	Attribut de sécurité « compact"	0xA1 4X 00 (voir note)	
						CHANGE REFERENCE DATA	Interdit
						VERIFY	SMI
						RESET RETRY COUNTER	Interdit
						RFU	Interdit
						RFU	Interdit
						PUT DATA	Interdit
						GET DATA	Libre
		9A	01	Nombre maximum d'essais autorisés		03	
		9B	01	Compteur d'essais restant		03	
		7F41	E	*Valeur du PIN*			
			Tag	**L**	**Description**		
			80	01	Taille maximum	06	
			81	01	Taille minimum	06	
			82	06	Valeur du PUK	*Typiquement dérivée d'une clé mère*	

Note: le 2^{e} octet de l'attribut de sécurité doit pointer sur le SE référençant ce jeu de clés (par exemple il prendra la valeur 43 si ce jeu de clés est référencé dans le SE 3).

4.1.3 - D001 – Identification porteur (EF.ID)

L'identification du porteur est constituée des informations suivantes :

- Le nom du porteur de la carte,
- Le prénom du porteur de la carte

Le nom et le prénom du porteur constitue des informations immuables (sauf dans le cas d'un mariage ou d'un divorce). Ces informations ne devraient pas être mises à jour.

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xD0 01	
		88	01	Identificateur de fichier court	Pas absolument nécessaire	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	**A définir en fonction de l'émetteur**	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	Interdit
					READ BINARY	SMI AA et PIN_Global

Seule l'opération de lecture est possible sur ce fichier. La lecture ne peut se faire que par une entité accréditée (Autorité Administrative) et sous contrôle du porteur.

Contenu :

Tag	L	Contenu			Type	Présence
65	7A	Groupe de données relatives au porteur (ISO7816-6 : Cardholder Related Data)				Obligatoire
		Tag	**L**	**Contenu**		
		80	3F	Nom du porteur	AL	Obligatoire
		81	2D	Prénom du porteur	AL	Obligatoire

4.1.4 - D002 – Adresse du porteur (EF.AD)

Ce fichier contient l'adresse du porteur. Contrairement au fichier d'identité ce fichier peut être mis à jour.

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xD0 02	
		88	01	Identificateur de fichier court	Pas absolument nécessaire	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	**A définir en fonction de l'émetteur**	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI Issuer et PIN Global
					READ BINARY	SMI AA et PIN_Global

Seules les opérations de lecture et de mise à jour sont possibles sur ce fichier. La lecture ne peut se faire que par une entité accréditée (Autorité Administrative) et sous contrôle du porteur. La mise à jour ne peut se faire que par l 'émetteur et sous contrôle du porteur.

Contenu :

Tag	L	Contenu			Type	Présence
65	7A	Groupe de données relatives au porteur (ISO7816-6 : Cardholder Related Data)				Obligatoire
		Tag	**L**	**Contenu**		
		83	var	Adresse du porteur	AL	Obligatoire

4.1.5 - FF8Axx – Jeu de Clés symétriques Autorité Administrative

Tag	L	Description	Valeur
FF8Axx	51	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	2	Longueur du DOUP	0x00 10
84	10	Nom de l'objet de sécurité	*Hérité des paramètres de la clé mère*
8C	3	Attribut de sécurité "compact"	0x89 00 00

RFU	Interdit
EXTERNAL AUTHENTICATE	Interdit
RFU	Interdit
MUTUAL AUTHENTICATE	Libre
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
9A	1	Nombre maximum d'erreurs autorisé	*Hérité des paramètres de la clé mère*
9B	1	Compteur d'erreurs	*Hérité des paramètres de la clé mère*
9C	2	Compteur d'utilisations	*Hérité des paramètres de la clé mère*
7F4B	27	*Valeur des clés*	

Tag	L	Description	Valeur
90	10	K MAC	*Dérivée de la clé mère*
91	10	K ENC	*Dérivée de la clé mère*
80	1	Algorithme d'usage	*Hérité des paramètres de la clé mère*

Ce jeu de clés doit permettre la lecture des fichiers identité et adresse du porteur.

4.2 - Environnements de sécurité

4.2.1 - FFFB06 – SE#6 SE dédié au PIN de déblocage du PIN global.

Tag	L	Description	Valeur
FFFB06	27	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 01
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*CRT Authentification PUK Global*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PIN (PUK)	0x02
80	01	Identifiant d'algorithme	0x00

4.2.2 - FFFB07 – SE#7 SE dédié à l'exploitation des fonctions crypto protégées sous PIN Global.

Tag	L	Description	Valeur
FFFB07	27	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 03
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*CRT Authentification PIN Global*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PIN	0x01
80	01	Identifiant d'algorithme	0x00

5 - ADF CIA Adèle

Afin de minimiser les besoins en environnement de sécurité (SE et SDO) ce DF ne contient que 2 fichiers : le fichier *EF.CIAInfo* et le fichier *EF.OD*. Ces deux fichiers n'ont, en effet, pas besoin d'être mis à jour. Les autres fichiers descripteurs conformes à la norme 7816-15 se trouvent dans l'application associée « Adèle » et bénéficient ainsi des environnements de sécurité de cette application.

Tag	**L**	**Description**			
62	17	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		82	01	Descripteur de fichier	0x38 (répertoire)
		84	0F	Nom de l'ADF (AID)	0xE8 28 BD 08 0F D2 50 00 00 04 41 64 E8 6C 65
		8C	01	Attribut de sécurité "compact"	0x00 DELETE FILE (sur le DF lui-même) Interdit TERMINATE FILE Interdit ACTIVATE FILE Interdit DEACTIVATE FILE Interdit CREATE FILE (DF) Interdit CREATE FILE (EF) / PUT DATA (SDO) Interdit

5.1 - Fichiers

5.1.1 - 5032 - EF.CIAInfo

Entête :

<table>
<tr><th>Tag</th><th>L</th><th colspan="4">Description</th><th colspan="2">Valeur</th></tr>
<tr><td>62</td><td>15</td><td colspan="6">File Control Parameter (FCP)</td></tr>
<tr><td colspan="2" rowspan="8"></td><td>Tag</td><td>L</td><td colspan="2">Description</td><td colspan="2">Valeur</td></tr>
<tr><td>80</td><td>02</td><td colspan="2">Nombre d'octets du fichier</td><td colspan="2">A définir</td></tr>
<tr><td>82</td><td>01</td><td colspan="2">Descripteur de fichier</td><td colspan="2">0x01 (EF transparent)</td></tr>
<tr><td>83</td><td>02</td><td colspan="2">Identificateur de fichier</td><td colspan="2">0x50 32</td></tr>
<tr><td>88</td><td>01</td><td colspan="2">Identificateur de fichier court</td><td colspan="2">0x90 (SFI=12)</td></tr>
<tr><td>8A</td><td>01</td><td colspan="2">Etat du cycle de vie</td><td colspan="2">A définir</td></tr>
<tr><td>8C</td><td>02</td><td colspan="2">Attribut de sécurité "compact"</td><td colspan="2">0x0100</td></tr>
<tr><td colspan="4"></td><td>DELETE FILE
TERMINATE FILE
ACTIVATE FILE
DEACTIVATE FILE
UPDATE BINARY
READ BINARY</td><td>Interdit
Interdit
Interdit
Interdit
Interdit
libre</td></tr>
</table>

Contenu :
Les tableaux suivants précisent les données devant être renseignées dans ce fichier

Données	Description		Obligatoire/ Optionnel
Version	Identifie la version de spécification ISO7816-15		Obligatoire
serialNumber	Identifiant unique de la carte. Cette donnée doit être présente si l'information est considérée comme non confidentielle (i.e. en lecture libre) sinon elle doit être omise		optionnel
Label	Contient des données d'identification de l'application pouvant être affichées par une application « terminal »		optionnel
cardflags	Donne des informations sur la carte :		Obligatoire
	readonly	Si la carte est en lecture seule	
	authRequired	Si des fonctions crypto. requièrent l'authentification du porteur	
	prnGeneration	Si la carte supporte la génération de quantité pseudo-aléatoire	
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l'application. Est composé des sous champs suivants :		Optionnel
	se	Désigne le numéro de SE	Obligatoire
	Owner	Dans le présent contexte désignera le propriétaire du jeu de clé pointé par le se	
	Aid	AID de l'application contenant le SE	
supportedAlgorithms	Décrit les différents algorithmes supportés par la carte ainsi que ses paramètres. Comprend les sous champs suivants :		
	reference	Identifiant unique dans l'application CIA	Obligatoire
	Algorithm	Identifiant d'algorithme selon PKCS#11	
	parameters	Paramètres d'utilisation de l'algorithme	
	supportedOperations	Liste des opérations pouvant être réalisées avec cet algorithme	
	objID	Identifiant type 'OID'	
	algRef	Identifiant de l'algorithme tel que géré par l'application IAS associée.	

Table 5-1 : EF.CIAInfo_Adèle : Description du contenu

Données	Valeur	
Version	2	
serialNumber	--	
Label	‘Adèle’	
cardflags	Donne des informations sur la carte :	
	readonly	Oui
	authRequired	Oui
	prnGeneration	Oui
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l’application.	
	se	2, 4, 7, 8, 9
	Owner	Pour les se #2, 4 et 9: OID PSCe (administrateur de l’application) Pour le se #8 : OID entité administrative possèdant le SignKeySet Pour le le se #7 : non renseigné
	Aid	Pour tous les se AID de l’application Adèle (i.e. 0xD2 50 00 00 04 41 64 E8 6C 65 01 01)
supportedAlgorithms	Voir tableau suivant	

Table 5-2 : EF.CIAInfo_Adèle : Valorisation des éléments (1ere partie)

Données	Valeur	
supportedAlgorithms#1	reference	1
	Algorithm	544 (SHA-1)
	parameters	NULL :NULL
	supportedOperations	hash
	objID	1 3 14 3 2 26
	algRef	16
supportedAlgorithms#2	reference	2
	Algorithm	592 (SHA-256)
	parameters	NULL :NULL
	supportedOperations	hash
	objID	2 16 840 1 101 3 4 2 1
	algRef	32
supportedAlgorithms#3	reference	3
	Algorithm	6 (Signature digitale avec RSA SHA-1 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 5
	algRef	18
supportedAlgorithms#4	reference	4
	Algorithm	64 (Signature digitale avec RSA SHA-256 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 11
	algRef	34
upportedAlgorithms#5	reference	5
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 1
	algRef	2
supportedAlgorithms#6	reference	6
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	decipher
	objID	1 2 840 113549 1 1 1
	algRef	26

Table 5-3 : EF.CIAInfo_Adèle : Valorisation des éléments (2ere partie) : Liste des algorithmes supportés

```
-- EF.CIAInfo
adele-1-EFCIAInfo CIAInfo ::= SEQUENCE
{  version v2, -- version de ISO/IEC 7816-15
       label "Adèle", -- peut contenir aussi manufacturerID[1]
       cardflags { authRequired, prnGeneration },
       seInfo
       { { se 2,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid '0xD2500000044164E86C650101' }, -- AID Adèle
         { se 4,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid '0xD2500000044164E86C650101' },
         { se 7,
       aid '0xD2500000044164E86C650101' },
         { se 8,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid '0xD2500000044164E86C650101' }
         { se 9,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid '0xD2500000044164E86C650101' }
       },
supportedAlgorithms
{
-- AlgID: 0x10, SHA-1
    { reference 1, -- unique référence dans CIA
    algorithm 544, -- calcul de condensat ref.PKCS#1,conforme ECC-2
    parameters NULL: NULL, -- type de paramètre NULL et valeur NULL
    supportedOperations {hash},
    objId {1 3 14 3 2 26},
    algRef 16 -- equivalent 0x10, algoID dans appli Adle, IAS V1.0
    },

-- Hash algorithm
-- AlgID: 0x40, SHA-256
    { reference 2, -- unique rfrence dans CIA
    algorithm 592, -- calcul de condens ref.PKCS#1,conforme ECC-2
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {hash},
    objId {2 16 840 1 101 3 4 2 1},
    algRef 32 -- equivalent 0x20, algoID IAS V1.0 Note that this is different from ECC-2
    },

-- Signature algorithm
-- Signature numrique RSA selon PKCS#1 avec SHA-1
    { reference 3, -- unique reference CIA, rfrence croise avec EF.PrKD
    algorithm 6, -- mcanisme RSA PKCS#1 avec SHA-1 = 0x12
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {compute-signature},
    objId {1 2 840 113549 1 1 5},
    algRef 18 -- equivalent 0x12, algoID dans appli Adle, IAS V1.0
},

-- Signature algorithm
-- Signature numrique RSA selon PKCS#1 avec SHA-256
    { reference 4, -- unique reference CIA, rfrence croise avec EF.PrKD
    algorithm 64, -- mcanisme RSA PKCS#1 avec SHA-256 = 0x22
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {compute-signature},
    objId {1 2 840 113549 1 1 11},
    algRef 34 -- equivalent 0x22, algoID dans appli Adle, IAS V1.0
},


-- C/S algorithm
-- Authentification Client/Serveur, signature RSA selon PKCS#1 sans info
```

[1] Le numéro de serie est géré via le fichier EF.DCOD. Le 'ManufacturerID' est optionnel mais pas vraiment utile dans le cadre de l'utilisation. Les problèmes doivent être remontés vers l'émetteur qui est identifié par l'EF.DIR.

```
-- abrges
-- AlgID: 0x02, C/S AUT
{ reference 5, -- unique reference CIA, rfrence croise avec EF.PrKD
        algorithm 1, -- mcanisme RSA PKCS#1 sans digest info = 0x02
        parameters NULL: NULL, -- type de parametre NULL et valeur NULL
        supportedOperations {compute-signature},
        objId {1 2 840 113549 1 1 1}, -- RSA with PKCS #1 padding
        algRef 2 -- equivalent 0x02, algoID dans appli Adle, IAS V1.0
},

-- Key decipherment algorithm
-- Key decipherment using RSA with PKCS #1 padding
-- AlgID: 0x02, C/S AUT
{ reference 6, -- unique reference CIA, rfrence croise avec EF.PrKD
        algorithm 1, -- mcanisme RSA PKCS#1 = 0x1A
        parameters NULL: NULL, -- type de parametre NULL et valeur NULL
        supportedOperations {decipher},
        objId {1 2 840 113549 1 1 1}, --  RSA with PKCS #1 padding
        algRef 26 -- equivalent 0x1A, algoID dans appli Adle, IAS V1.0
},
}}
```

5.1.2 - 5031 - EF.OD

Entête :

<table>
<tr><th>Tag</th><th>L</th><th colspan="3">Description</th><th>Valeur</th></tr>
<tr><td>62</td><td>18</td><td colspan="4">File Control Parameter (FCP)</td></tr>
<tr><td colspan="2"></td><td>Tag</td><td>L</td><td>Description</td><td>Valeur</td></tr>
<tr><td colspan="2"></td><td>80</td><td>02</td><td>Nombre d'octets du fichier</td><td>0x60</td></tr>
<tr><td colspan="2"></td><td>82</td><td>01</td><td>Descripteur de fichier</td><td>0x01 (EF transparent)</td></tr>
<tr><td colspan="2"></td><td>83</td><td>02</td><td>Identificateur de fichier</td><td>0x50 31</td></tr>
<tr><td colspan="2"></td><td>88</td><td>01</td><td>Identificateur de fichier court</td><td>0x88(SFI=11)</td></tr>
<tr><td colspan="2"></td><td>85</td><td>01</td><td>Niveau de renforcement</td><td>0x00</td></tr>
<tr><td colspan="2"></td><td>8A</td><td>01</td><td>Etat du cycle de vie</td><td>0x05</td></tr>
<tr><td colspan="2"></td><td>8C</td><td>02</td><td>Attribut de sécurité "compact"</td><td>0x01 00
DELETE FILE — Interdit
TERMINATE FILE — Interdit
ACTIVATE FILE — Interdit
DEACTIVATE FILE — Interdit
UPDATE BINARY — Interdit
READ BINARY — Libre</td></tr>
</table>

Contenu :

```
-- le Path étendu est en accord avec l'amendement n°2 de ISO/IEC WD 7816-15:2004/AM2 version draft
du 14 mars 2007.
-- le champ AID étant présent, le chemin spécifié est un chemin relatif par rapport au DF
sélectionné -- par cet AID

privateKeys :
 path :{   AID ‘0xD2500000044164E86C0101
           efidOrPath '0x7002'
       },


certificates :
 path :{   AID‘0xD2500000044164E86C0101
           efidOrPath '0x7005'
      },


dataContainerObjects :
 path :{   AID ‘0xD2500000044164E86C0101
           efidOrPath '0x7006'
      },


authObjects :
 path :{   AID ‘0xD2500000044164E86C0101
           efidOrPath '0x7001'
```

```
Ce qui donne au format BER-TLV :
T=A0 L=0x16
    T=30 L=0x14
        T=A1 L=0x12
            T=4F L=0x0C
                0xD2 50 00 00 04 41 64 E8 6C 65 01 01
            T=04 L=02
                70 02
T=A4 L=0x16
    T=30 L=0x14
        T=A1 L=0x12
            T=4F L=0x0C
                0xD2 50 00 00 04 41 64 E8 6C 65 01 01
            T=04 L=2
                70 05
T=A7 L=0x16
    T=30 L=0x14
        T=A1 L=0x12
            T=4F L=0x0C
                0xD2 50 00 00 04 41 64 E8 6C 65 01 01
            T=04 L=02
                70 06
T=A8 L=0x16
    T=30 L=0x14
        T=A1 L=0x12
            T=4F L=0x0C
                0xD2 50 00 00 04 41 64 E8 6C 65 01 01
            T=04 L=02
                70 01
```

6 - ADF Adèle

<table>
<tr><th>Tag</th><th>L</th><th colspan="3">Description</th><th>Valeur</th></tr>
<tr><td>62</td><td>15</td><td colspan="4">File Control Parameter (FCP)</td></tr>
<tr><td colspan="2" rowspan="5"></td><td>Tag</td><td>L</td><td>Description</td><td>Valeur</td></tr>
<tr><td>82</td><td>01</td><td>File Descriptor</td><td>0x38 (répertoire)</td></tr>
<tr><td>84</td><td>05</td><td>AID of the ADF</td><td>0xD2 50 00 00 04 41 64 E8 6C 65 01 01</td></tr>
<tr><td>8A</td><td>01</td><td>Life Cycle Status</td><td>A définir</td></tr>
<tr><td>8C</td><td>06</td><td>Compact Security Attributs</td><td>0x3E 44 44 44 44 44
DELETE FILE (sur le DF lui-même) : Interdit
TERMINATE FILE : SMI PSCe
ACTIVATE FILE : SMI PSCe SMI PSCe
DEACTIVATE FILE : SMI PSCe
CREATE FILE (DF) : SMI PSCe
CREATE FILE (EF) / PUT DATA (SDO) : SMI PSCe</td></tr>
</table>

Les attributs de sécurité se réfèrent au SE de SecureMessaging en intégrité uniquement pointant sur les clés d'administration de l'application. Ces clés sont gérées par un PSCe.

6.1 - Fichiers/Objets d'authentification du porteur pour la signature

Un PIN dédié à la protection de la signature est obligatoire pour pouvoir atteindre le niveau de signature qualifiée appelé *** (‘trois étoiles’).

Dans le cas de signature ‘*’ ou ‘**’, la protection se fait à l'aide du PIN Global, cependant, le statut de sécurité associé au PIN Global ne sera pas remis à zéro après une signature.

Par exemple, la gestion du PIN de signature pourrait se faire comme suit :

En fin de personnalisation, le PIN de Signature est bloqué. Il est nécessaire de débloquer le PIN. Le déblocage du PIN est réalisé à l'aide d'un code PUK qui est calculé par un PSCe et envoyé à la carte sous SecureMessaging. Le porteur doit alors compléter le déblocage en introduisant un nouveau code PIN de signature. Celui-ci sera introduit sans SecureMessaging afin de laisser le porteur maître de la valeur de son PIN de Signature.

Le code PUK n'est valide qu'une seule fois, aussi pour pouvoir débloquer le PIN de signature plusieurs fois, il est nécessaire de personnaliser plusieurs codes PUK dans l'application. Il appartient à l'application « Adèle » de définir le nombre de fois le code PIN de Signature pourra être débloqué avant remplacement de la carte. Ce nombre peut éventuellement varier en fonction du type de carte et la durée de validité correspondante.

6.1.1 - FF8101 - PIN dédié à la protection de la Signature

Caractéristique de l'Objet :

Tag	L	Description				Valeur	
FF8101	2E	*Référence de l'objet*					
		Tag	**L**	**Description**		**Valeur**	
		E2	15	*DOCP*			
			Tag	**L**	**Description**	**Valeur**	
			80	02	Longueur du DOUP	0x00 06	
			84	08	Nom de l'objet de sécurité	"PIN Sign"	
			8C	05	Attribut de sécurité "compact"	0xF1 18 00 19 00	
						CHANGE REFERENCE DATA — PIN Sign VERIFY — Libre RESET RETRY COUNTER — Auth Code PUK RFU — Interdit RFU — Interdit PUT DATA — Interdit GET DATA — Libre	
		9A	01	Nombre maximum d'essais autorisés		0x05	
		9B	01	Compteur d'essais		0x00 (code bloqué)	
		7F41	0E	*Valeur du PIN*			
			Tag	**L**	**Description**	**Valeur**	
			80	01	Taille maximum	0x06	
			81	01	Taille minimum	0x06	
			82	06	Valeur du PIN	0x303030303030	

Le PIN de Signature est de 6 caractères décimaux pour être conforme au Profil de Protection « Secure Signature Creation Device ».

6.1.2 - FF8111 – Unblock PIN Code #1

Tag	L	Description	Valeur
FF8111	39	*Référence de l'objet*	
		Tag **L** **Description**	
		E2 1B	*DOCP*
		Tag **L** **Description**	
		80 02 Longueur du DOUP	00 08
		84 10 Nom de l'objet de sécurité	*Hérité des paramètres de la clé mère*
		8C 03 Attribut de sécurité « compact"	0xA1 44 00 CHANGE REFERENCE DATA — Interdit VERIFY — SMI PSCe RESET RETRY COUNTER — Interdit RFU — Interdit RFU — Interdit PUT DATA — Interdit GET DATA — Libre
		9A 01 Nombre maximum d'essais autorisés	01
		9B 01 Compteur d'essais restant	01
		9C 02 Usage Counter	0x0001
		7F41 10	*Valeur du PIN*
		Tag **L** **Description**	
		80 01 Taille maximum	08
		81 01 Taille minimum	08
		82 08 Valeur du PUK	*Dérivée de la clé mère*

6.1.3 - FF8112 – Unblock PIN Code #2

Idem bloc précédent avec pour seules modifications :

- L'identification de l'objet 'FF8112'
- La valeur associée au Tag '84'
- La valeur associée au Tag '82' sous le Tag '7F41'

6.1.4 - FF8113 – Unblock PIN Code #3

Idem bloc précédent avec pour seules modifications :

- L'identification de l'objet 'FF8113'
- La valeur associée au Tag '84'
- La valeur associée au Tag '82' sous le Tag '7F41'

6.2 - Les fichiers/objets d'administration de l'application

Les fichiers ou objets d'administration sont décrits dans ce paragraphe. Les différents objets décrits sont :

Les environnements de sécurité. Ils sont au nombre de trois pour un profil * ou **, et au nombre de cinq pour un profil *** :

- Le SE#2 dédié à la gestion administrative de l'application quand les protections font appel à l'authentification mutuelle, l'intégrité, la confidentialité. Les clés correspondantes sont sous contrôle d'un PSCe (PSCe_KeySet).
- Le SE#4 dédié à la gestion administrative de l'application quand les protections font appel à l'authentification mutuelle, l'intégrité et/ou du porteur par PIN Global. Les clés correspondantes sont sous contrôle d'un PSCe (PSCe_KeySet).
- Le SE#7 dédié à la gestion des protections des fonctions cryptographiques mises en œuvre par l'application (hors administration). Cet environnement ne référence que le PIN_Global.
- Le SE#8 dédié à la gestion des protection de la signature qualifiée (profil ***). Cet environnement fait référence au PIN de signature (PIN_Sign) et au jeu de clé nécessaire (Sign_KeySet) à la gestion de l'intégrité de la demande de signature (PSO Compute).
- Le SE#9 dédié à la gestion du déblocage du PIN

6.2.1 - FICHIER SERIAL NUMBER

Pour des raisons d'interopérabilité et de compatibilité avec le standard européen ECC2, ce fichier contient le numéro unique d'identification de la carte. Il contient l'information « Numéro de Série » comme défini dans la spécification IAS et qui est recouvrable via la commande GetData sous le Tag '5A'.

Entête :

Tag	L	Description			Valeur	
62	15	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	0x0015	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xD0 03	
		88	01	Identificateur de fichier court	0x10 (SFI = 02)	
		8A	01	Etat du cycle de vie	0x05	
		8C	02	Attribut de sécurité "compact"	0x01 00[2]	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	Interdit
					READ BINARY	libre

Seule l'opération de lecture est possible sur ce fichier. La lecture est libre.
Contenu :

Tag	L	Contenu	Type	Présence
5A	13	« numéro unique d'identification du porteur ». Voir [IAS][3]	N	Obligatoire

La gestion du numéro de série adoptée est identique à celle utilisée pour les applications bancaires qui se base sur l'utilisation de l'objet PAN définit par l'ISO 7816-6 (Tag '5A').
Le PAN est décrit au sein de la norme ISO7812 :

	Définition du PAN ISO 7812				
Longueur	**9 digits**			**16 digits**	**1 digit**
Éléments	IIN Issuer Identification Number			Identificateur unique de carte	Clé de luhn
	MII	Pays	Identificateur émetteur		

[2] Les protections de la donnée recouvrable via GetData ou par lecture de ce fichier doivent être identiques.
[3] La valeur doit être identique à celle recouvrable via le GetData.

6.2.2 - FFFB02 – SE#2 dédié à la gestion administrative de l'application par PSCe

Ce SE doit être utilisé pour une protection en Secure Messaging faisant appel à une authentification mutuelle, de l'intégrité et de la confidentialité.

Tag	L	Description	Valeur
FFFB02	3D	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 03
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*Authentification Mutuelle symétrique PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x C0
83	01	Référence du jeu de clés symétriques d'authentification	0x 82 (PSCe)
80	01	Identifiant d'algorithme	0x 1C

Tag	L	Description	Valeur
B4	09	*CRT de SMI PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82
80	01	Identifiant d'algorithme	0x1C

Tag	L	Description	Valeur
B8	09	*CRT de SMC PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82 (Voir CRT AT)
80	01	Identifiant d'algorithme	0x1C

6.2.3 - FFFB04 - SE#4 dédié à la gestion administrative de la carte par un PSCe – Intégrité Uniquement

Ce SE doit être utilisé pour des besoins de protection en intégrité seule.

Tag	L	Description	Valeur
FFFB02	32	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 02
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00 RFU Interdit RFU Interdit RFU Interdit RFU Interdit MANAGE SE Interdit PUT DATA Interdit GET DATA Libre

Tag	L	Description	Valeur
A4	09	*Authentification Mutuelle symétrique*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x C0
83	01	Référence du jeu de clés symétriques d'authentification	0x 82 (PSCe)
80	01	Identifiant d'algorithme	0x 1C

Tag	L	Description	Valeur
B4	09	*CRT de SMI PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82
80	01	Identifiant d'algorithme	0x1C

6.2.4 - FFFB07 – SE#7 SE dédié à l'exploitation des fonctions crypto protégée sous PIN Global.

Ce SE doit être utilisé pour les clés d'authentification et de chiffrement pour les profils *, ** ou *** ; et pour les clés de signature dans le cas de profils * ou **.

Tag	L	Description	Valeur
FFFB07	27	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 01
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*CRT Authentification PIN Global*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PIN	0x01
80	01	Identifiant d'algorithme	0x00

Le SE ne référence pas de CRT d'authentification asymétrique, de déchiffrement, ou de signature car le SE courant sera construit au fur et à mesure des besoins de l'application.

6.2.5 - – SE#8 SE dédié à l'exploitation du profil *** pour la signature

Tag	L	Description	Valeur
FFFB08	3D	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 03
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*CRT Authentification PIN_Sign*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PIN	0x81
80	01	Identifiant d'algorithme	0x00

Tag	L	Description	Valeur
A4	09	*Authentification Mutuelle symétrique SignKeySet*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0xC0
83	01	Référence du jeu de clés symétriques	0x83 (SignKeySet)
80	01	Identifiant d'algorithme	0x1C

Tag	L	Description	Valeur
B4	09	*CRT de SMI SignKeySet*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques	0x83
80	01	Identifiant d'algorithme	0x1C

6.2.6 - – SE#9 SE dédié au déblocage du PIN de Signature

Tag	L	Description	Valeur
FFFB09	2D	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 01
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	0F	*CRT Authentification PUK*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PUK #1	0x91
83	01	Référence du PUK #2	0x92
83	01	Référence du PUK #3	0x93
80	01	Identifiant d'algorithme	0x00

6.2.7 - FF8A02 – Jeu de Clés symétriques PSCe

Tag	L	Description	Valeur
FF8A02	51	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	2	Longueur du DOUP	0x00 10
84	10	Nom de l'objet de sécurité	*Hérité des paramètres de la clé mère*
8C	3	Attribut de sécurité "compact"	0x89 00 00

RFU	Interdit
EXTERNAL AUTHENTICATE	Interdit
RFU	Interdit
MUTUAL AUTHENTICATE	Libre
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
9A	1	Nombre maximum d'erreurs autorisé	*Hérité des paramètres de la clé mère*
9B	1	Compteur d'erreurs	*Hérité des paramètres de la clé mère*
9C	2	Compteur d'utilisations	*Hérité des paramètres de la clé mère*
7F4B	27	*Valeur des clés*	

Tag	L	Description	Valeur
90	10	K MAC	*Dérivée de la clé mère*
91	10	K ENC	*Dérivée de la clé mère*
80	1	Algorithme d'usage	*Hérité des paramètres de la clé mère*

6.2.8 - FF8A03 – Jeu de Clés symétriques dédiées à la gestion de la signature qualifiée

Tag	L	Description	Valeur
FF8A03	51	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	2	Longueur du DOUP	0x00 10
84	10	Nom de l'objet de sécurité	*Hérité des paramètres de la clé mère*
8C	3	Attribut de sécurité "compact"	0x89 00 00

RFU	Interdit
EXTERNAL AUTHENTICATE	Interdit
RFU	Interdit
MUTUAL AUTHENTICATE	Libre
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
9A	1	Nombre maximum d'erreurs autorisé	*Hérité des paramètres de la clé mère*
9B	1	Compteur d'erreurs	*Hérité des paramètres de la clé mère*
9C	2	Compteur d'utilisations	*Hérité des paramètres de la clé mère*
7F4B	27	*Valeur des clés*	

Tag	L	Description	Valeur
90	10	K MAC	*Dérivée de la clé mère*
91	10	K ENC	*Dérivée de la clé mère*
80	1	Algorithme d'usage	*Hérité des paramètres de la clé mère*

6.3 - Les fichiers ISO 7816-15

6.3.1 - 7001 - EF.AOD

Ce fichier décrit les objets utilisés lors d'une authentification du porteur ou d'une authentification externe.
Entête :

Tag	L	Description			Valeur
62	16	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		80	02	Nombre d'octets du fichier	*A définir*
		82	01	Descripteur de fichier	0x01 (EF transparent)
		83	02	Identificateur de fichier	0x70 01
		88	01	Identificateur de fichier court	NA
		8A	01	Etat du cycle de vie	0x05
		8C	03	Attribut de sécurité "compact"	0x03 44 00 DELETE FILE : Interdit TERMINATE FILE : Interdit ACTIVATE FILE : Interdit DEACTIVATE FILE : Interdit UPDATE BINARY : SMI PSCe READ BINARY : Libre

Contenu :

Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PIN de la carte »
	authId	Reference to Class.authId du PUK	Obligatoire	'02'
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'C1'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PIN Global)
		change-disable[4]		*A voir avec l'émetteur*
		Unblock disable		*A voir avec l'émetteur*
		initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Faux
		soPassword		Faux
		Disabble-allowed		Faux
		Integrity-protected		Faux
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'04'
	stroredLength	Longueur du PIN	obligatoire	'04'
	maxLength	Longueur Max du PIN	Optionnel	'04'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	01

Table 6-1 : EF.AOD_Adèle : Description de l'objet PIN_Global

[4] A voir avec l'émetteur

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PUK pour PIN de la carte »
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'02'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PUK global)
		change-disable		Dépend du statut CHANGE REFERENCE DATA du PUK Global. Voir section 4.1.2 -
		Unblock disable		Vrai
		initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Vrai
		soPassword		Faux
		Disable-allowed		Faux
		Integrity-protected		Dépend du statut VERIFY (SMI ou non) du PUK Global .Voir section 4.1.2 -
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'06'
	stroredLength	Longueur du PIN	obligatoire	'06'
	maxLength	Longueur Max du PIN	Optionnel	'06'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	02

Table 6-2 : EF.AOD_Adèle : Description de l'objet PUK_Global

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PIN de signature»
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'81'
Type	pwdFlags	case-sensitive	obligatoire	Faux
		Local		Vrai (PIN local)
		change-disable		Vrai
		Unblock disable		faux
		initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Faux
		soPassword		Faux
		Disabble-allowed		Faux
		Integrity-protected		Faux
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'06'
	stroredLength	Longueur du PIN	obligatoire	'06'
	maxLength	Longueur Max du PIN	Optionnel	'06'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	81

Table 6-3 : EF.AOD_Adèle : Description de l'objet PIN_Sign (PIN de signature)

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PUK #1»
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'91'
Type	pwdFlags	case-sensitive	obligatoire	Faux
		Local		Vrai (PUK local)
		change-disable		Vrai
		Unblock disable		Vrai
		initialized		Vrai
		Needs-padding		Faux
		unblockingPassword		Vrai
		soPassword		Faux
		Disabble-allowed		Faux
		Integrity-protected		Vrai
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Utf8
	minLength	Longueur Min du PIN	obligatoire	'16'
	stroredLength	Longueur du PIN	obligatoire	'16'
	maxLength	Longueur Max du PIN	Optionnel	'16'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	'91'

Table 6-4 : EF.AOD_Adèle : Description d'un objet PUK de Signature

Les PUK étant au nombre de trois, il est nécessaire de coder trois objets de ce type. Pour les PUK#2 et #3 les valeurs à modifier sont le label (respectivement « PUK #2» et « PUK #3») authID (respectivement '92' et '93') et pwdReference (respectivement '92' et '93').

6.3.2 - 7002 - EF.PrKD

Ce fichier contient une description des clés privées utilisées lors de services cryptographiques.

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 02	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :

Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé d'authentification »**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide (correspond à pas de compteur)
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	encipher	Obligatoire	non
		decipher		non
		sign		Oui
		signRecover		non
		keyEncipher		non
		verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		non
	accessFlags	sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'01'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	'05' RSA format PKCS#1 sans digestInfo
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 6-5 : EF.PrKD_Adèle : Description de l'objet Clé RSA d'authentification

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé de signature»**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide pour les profils * et **, '01' pour le profil ***
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	encipher	Obligatoire	non
		decipher		non
		sign		Oui
		signRecover		non
		keyEncipher		non
		verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		**Oui** si la clé est générée "on board" **non** sinon
	accessFlags	sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'02'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	Pour les profils * et ** : '05' RSA format PKCS#1 sans digestInfo Pour le profil *** : '03' si DSI avec RSA et SHA-1 '04' si DSI avec RSA et SHA-256
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 6-6 : EF.PrKD_Adèle : Description de l'objet Clé RSA de signature

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé de déchiffrement de clé»**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide (pas de reset du PIN après utilisation)
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	encipher	Obligatoire	non
		decipher		non
		sign		non
		signRecover		non
		keyEncipher		non
		keyDecipher		oui
		verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		non
	accessFlags	sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'03'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	'06' RSA format PKCS#1 sans digestInfo
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 6-7 : EF.PrKD_Adèle : Description de l'objet Clé RSA de déchiffrement

AccessMode		Security Condition		
Field	Operation	Clé d'authentification	Clé de signature	Clé de déchiffrement
Read	-			
Update	Update or Generate Key Pair	NA [5]	NA	NA
Execute	InternalAuth, PSOCompute, PSODecipher	'C1'	Pour les profils * et ** AuthID = 'C1' Pour le profil *** AuthID=AND { AuthID='81' AuthReference= {AuthMethod = secureMessaging, seEntifier='08' }	'C1'
Delete	-			

Table 6-8 : EF.PrKD_Adèle : accessControlRules pour les clés RSA

[5] voir Flag « modifiable »

6.3.3 - 7003 -EF.SK

Ce fichier est destiné à décrire les objets cryptographiques symétriques utilisés à des fins de « device authentication ». L'application n'utilise des jeux de clé symétriques qu'à des fins de « secure-messaging », aussi ce fichier n'est pas supporté par les profils.

6.3.4 - 7004 - Description des clés publiques (EF.PuKD)

Ce fichier n'est a priori pas nécessaire dans la mesure où les clés publiques présentes dans la carte ne sont pas utilisées afin d'exploiter des certificats vérifiables par la carte (Card Verficable Certificates) mais uniquement pour le support de la génération de clé dans la carte.

6.3.5 - 7005 - Description des certificats (EF.CD) (P)

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 05	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :
Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/ Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**Voir Tableau ci-dessous**
	accessControlRules		obligatoire	
Class	iD	Identifiant Unique		**Voir règle de génération des Id uniques**
Type	Path	Chemin d'accès au certificat		**Voir Tableau ci-dessous**

Table 6-9 : EF.CD_Adèle : Description de l'objet Certificat

Label	iD	path[6]
« Certificat d'authentification »		'A001'
« Certificat de signature »		'A002'
« Certificat de déchiffrement de clé»		'A003'

Table 6-10 : EF.CD_Adèle : Liste des certificats (non CA) devant apparaître dans EF.CD

AccessMode		Security Condition
Field	Operation	
Read	read	always
Update	Update	authReference { authMethod=secureMessaging seIdentifier=4}
Execute	-	
Delete	-	

Table 6-11 : EF.CD_Adèle : accessControlRules pour les certificats

[6] La référence est relative par rapport au DF courant

6.3.6 - 7006 - EF.DCOD

Ce fichier fournit les informations nécessaires à la gestion des objets non cryptographiques et plus particulièrement il fournit les pointeurs vers les fichiers identité et adresse du porteur.

Entête :

Tag	L	Description			Valeur
62	16	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		80	02	Nombre d'octets du fichier	*A définir*
		82	01	Descripteur de fichier	0x01 (EF transparent)
		83	02	Identificateur de fichier	0x70 06
		88	01	Identificateur de fichier court	NA
		8A	01	Etat du cycle de vie	0x05
		8C	03	Attribut de sécurité "compact"	0x03 44 00

DELETE FILE	Interdit
TERMINATE FILE	Interdit
ACTIVATE FILE	Interdit
DEACTIVATE FILE	Interdit
UPDATE BINARY	SMI PSCe
READ BINARY	Libre

Contenu :

Pour fournir les informations, des éléments de description de type « opaqueDO » sont utilisés. Les informations qui sont décrites dans ce fichier sont :
Le fichier EF.Id contenant l'identité du porteur.
Le fichier EF.Ad contenant l'adresse du porteur

ECC2 décrit de la même manière le numéro de série. Le numéro de série se trouve donc dans un fichier. Attention, il y a divergence sur ce point avec IAS.

Les tableaux ci-après décrivent les éléments de données devant figurer dans le fichier ainsi que les attributs associés devant être décrits. La mise en forme au format « ISO 7816-15 » doit être faite après avoir renseigné les différents attributs.

Attributs	Item	Description	
CommonObject	Label	Voir Tableau ci-dessous	Obligatoire
	accessControlRules	Décrit les conditions d'accès au fichier	Obligatoire
Class	ApplicationName	AID de l'application adèle (??)	Obligatoire
Type	ExtendedPath	Chemin d'accès au fichier	Obligatoire

Table 6-12 : EF.DCOD_Adèle : Attributs des objets "opaqueDO"

Label	path	Fichier	Description
« EF.ID »	'3F00D001'[7]	EF.Ident	Contient l'identité du porteur
« EF.AD »	'3F00D002'	EF.Adresse	Contient l'adresse du porteur
« EF.SN »	'D003'	EF.SerialNumber	Contient le Numéro unique d'identification du porteur

Table 6-13 : EF.DCOD_Adèle : Liste des fichiers référencés dans le fichier DCOD

[7] Dans le cas où la carte ne supporte pas de MF, il est nécessaire d'utiliser un « Path étendu » pour pointer sur les fichiers EF_ID, EF_AD voire EF_SN.

6.4 - Les fichiers/objet cryptographiques de l’application

Dans cette implémentation, il a été choisi de supporter un fichier par type de certificat.

6.4.1 - A001 - Certificat d'authentification Client /Serveur

Entête :

Tag	L	Description			Valeur	
62	1D	File Control Parameter (FCP)				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xA0 01	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00	
					DELETE FILE	SMI PSCe
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :
Il est préconisé d’inscrire le certificat au format binaire.

6.4.2 - A002 - Certificat de signature porteur

Entête :

Tag	L	Description			Valeur	
62	1D	File Control Parameter (FCP)				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xA0 02	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00	
					DELETE FILE	SMI PSCe
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :
Il est préconisé d'inscrire le certificat au format binaire.

6.4.3 - A003 - Certificat de chiffrement

Entête :

Tag	L	Description			Valeur	
62	1D	File Control Parameter (FCP)				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xA0 03	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00	
					DELETE FILE	SMI PSCe
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :
Il est préconisé d'inscrire le certificat au format binaire.

6.4.4 - FF9001 – Clé Privée dédiée à l'authentification (*, **, ***) sans génération par la carte)

Tag	L	Description	Valeur
FF9001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA3 17 C2 00 PSO SIGN : Interdit INTERNAL AUTHENTICATE : PIN Global PSO DECIPHER : Interdit GENERATE KEY PAIR : interdit RFU : Interdit PUT DATA : SMIC PSCe GET DATA : Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF[8]
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction d'authentification est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[8] Le compteur d'utilisation est positionné au maximum, mais peut être mis à une autre valeur en fonction de l'application
[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.5 - FF9001 – Clé Privée dédiée à l'authentification (*, **, ***) avec génération par la carte)

Tag	L	Description	Valeur
FF9001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA9 17 C4 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	PIN Global
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
9C	2	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	Non renseigné en perso
93	80	q	Non renseigné en perso
94	80	q^{-1} mod p	Non renseigné en perso
95	80	dp	Non renseigné en perso
96	80	dq	Non renseigné en perso
80	01	Algorithme d'usage	0x02

La fonction d'authentification est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.6 - FF9002 – Clé Privée dédiée à la signature (*, **) sans génération de clé par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA2 17 C2 00 PSO SIGN — Interdit INTERNAL AUTHENTICATE — PIN Global PSO DECIPHER — Interdit GENERATE KEY PAIR — interdit RFU — Interdit PUT DATA — SMIC PSCe GET DATA — Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction de signature est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.7 - FF9002 – Clé Privée dédiée à la signature (*, **) avec génération par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA9 17 C4 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	PIN Global
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
9C	2	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	Non renseigné en perso
93	80	q	Non renseigné en perso
94	80	q^{-1} mod p	Non renseigné en perso
95	80	dp	Non renseigné en perso
96	80	dq	Non renseigné en perso
80	01	Algorithme d'usage	0x02

La fonction de signature est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.8 - FF9002 – Clé Privée de signature (*** sans génération de clé par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xC3 D8 C2 00

PSO SIGN	PIN_Sign et SMI SignKeySet
INTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	Interdit
GENERATE KEY PAIR	Interdit
RFU	Interdit
PUT DATA	SMIC PSCe
GET DATA	Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Oui
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de signature est protégée par le PIN de Signature. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.9 - FF9002 – Clé Privée de signature (*** avec génération de clé par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xC9 D8 C4 00

PSO SIGN	PIN_Sign et SMI SignKeySet
INTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Oui
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de signature est protégée par le PIN de Signature. La génération de la valeur de la clé se fait sous contrôle du PSCe. La commande *GenerateKeyPair* doit être protégée en intégrité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.10 - FF9003 – Clé Privée de Chiffrement (* ou ** ou *** sans génération de clé par la carte)

Tag	L	Description	Valeur
FF9003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	
8C	04	Attribut de sécurité "compact"	0x93 17 C2 00 PSO SIGN : Interdit INTERNAL AUTHENTICATE : Interdit PSO DECIPHER : PIN Global GENERATE KEY PAIR : Interdit RFU : Interdit PUT DATA : SMIC PSCe GET DATA : Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Oui
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de chiffrement est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.11 - FF9003 – Clé Privée de Chiffrement (* ou ** ou *** avec génération de clé par la carte)

Tag	L	Description	Valeur
FF9003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0x99 17 C4 00 PSO SIGN : Interdit INTERNAL AUTHENTICATE : Interdit PSO DECIPHER : PIN Global GENERATE KEY PAIR : SMI PSCe RFU : Interdit PUT DATA : Interdit GET DATA : Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Oui
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de chiffrement est protégée par authentification du porteur sous PIN global. La génération de la valeur de la clé se fait sous contrôle du PSCe. La commande *GenerateKeyPair* doit être protégée en intégrité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

FFA001 – Clé publique d'authentification
La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	Taille du modulo
84	10	Nom de l'objet de sécurité	*A définir*
8C	03	Attribut de sécurité "compact"	0x89 C4 00

PSO SIGN	Interdit
EXTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.12 - FFA002 – Clé publique de signature

La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	Taille du modulo
84	10	Nom de l'objet de sécurité	*A définir*
8C	03	Attribut de sécurité "compact"	0x89 C4 00

PSO SIGN	Interdit
EXTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

6.4.13 - FFA003 – Clé publique de chiffrement

La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur	
80	02	Longueur du DOUP	Taille du modulo	
84	10	Nom de l'objet de sécurité	*A définir*	
8C	03	Attribut de sécurité "compact"	0x89 C4 00	
			PSO SIGN	Interdit
			EXTERNAL AUTHENTICATE	Interdit
			PSO DECIPHER	Interdit
			GENERATE KEY PAIR	SMI PSCe
			RFU	Interdit
			PUT DATA	interdit
			GET DATA	Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

7 - ADF CIA Adèle Générique

Ce DF contient l'ensemble des fichiers nécessaires à l'exploitation des fonctions cryptographiques via une couche logicielle PKCS#11 ou MS CAPI. De plus pour satisfaire les besoins de mise à jour sous PKCS#11, les protections ne font appel qu'au PIN global.
Au niveau du DF, les protections sont données dans le tableau ci-après. L'effacement du DF est interdit de même que la création d'autres DF.

<table>
<tr><th>Tag</th><th>L</th><th colspan="3">Description</th><th colspan="2">Valeur</th></tr>
<tr><td>62</td><td>1B</td><td colspan="5">File Control Parameter (FCP)</td></tr>
<tr><td colspan="2" rowspan="4"></td><th>Tag</th><th>L</th><th>Description</th><th colspan="2">Valeur</th></tr>
<tr><td>82</td><td>01</td><td>Descripteur de fichier</td><td colspan="2">0x38 (répertoire)</td></tr>
<tr><td>84</td><td>0F</td><td>Nom de l'ADF (AID)</td><td colspan="2">0xE8 28 BD 08 0F TBC</td></tr>
<tr><td>8C</td><td>05</td><td>Attribut de sécurité "compact"</td><td colspan="2">0x3A 17 17 17 17
DELETE FILE (sur le DF lui-même) : Interdit
TERMINATE FILE : PIN Global
ACTIVATE FILE : PIN Global
DEACTIVATE FILE : PIN Global
CREATE FILE (DF) : Interdit
CREATE FILE (EF) / PUT DATA (SDO) : PIN Global</td></tr>
</table>

7.1 - Fichiers 7816-15

7.1.1 - 5032 - EF.CIAInfo

Entête :

Tag	L	Description			Valeur	
62	15	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x50 32	
		88	01	Identificateur de fichier court	0x90 (SFI=12)	
		8A	01	Etat du cycle de vie	*A définir*	
		8C	02	Attribut de sécurité "compact"	0x03 17 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	PIN_Global
					READ BINARY	libre

Contenu :
Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Données	Description		Obligatoire/ Optionnel
Version	Identifie la version de spécification ISO7816-15		Obligatoire
serialNumber	Identifiant unique de la carte. Cette donnée doit être présente si l'information est considérée comme non confidentielle (i.e. en lecture libre) sinon elle doit être omise		optionnel
Label	Contient des données d'identification de l'application pouvant être affichées par une application « terminal »		optionnel
Cardflags	Donne des informations sur la carte :		Obligatoire
	readonly	Si la carte est en lecture seule	
	authRequired	Si des fonctions crypto. requièrent l'authentification du porteur	
	prnGeneration	Si la carte supporte la génération de quantité pseudo-aléatoire	
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l'application. Est composé des sous champs suivants :		Optionnel
	se	Désigne le numéro de SE	Obligatoire
	Owner	Dans le présent contexte désignera le propriétaire du jeu de clé pointé par le se	
	Aid	AID de l'application contenant le SE	
supportedAlgorithms	Décrit les différents algorithmes supportés par la carte ainsi que ses paramètres. Comprend les sous champs suivants :		
	reference	Identifiant unique dans l'application CIA	Obligatoire
	Algorithm	Identifiant d'algorithm selon PKCS#11	
	parameters	Paramètres d'utilisation de l'algorithme	
	supportedOperations	Liste des opérations pouvant être réalisées avec cet algorithme	
	objID	Identifiant type 'OID'	
	algRef	Identifiant de l'algorithme tel que géré par l'application IAS associée.	

Table 7-1 : EF.CIAInfo_Adèle Générique : Description

Données	Valeur	
Version	2	
serialNumber	--	
Label	'Générique PKCS#11'	
Cardflags	Donne des informations sur la carte :	
	readonly	Non
	authRequired	Oui
	prnGeneration	Oui
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l'application.	
	se	7
	Owner	Pour le se #7 : non renseigné
	Aid	Non renseigné car dans le DF courant
supportedAlgorithms	Voir tableau suivant	

Table 7-2 : EF.CIAInfo_Adèle Générique : Valorisation des éléments (1ere partie)

Données	Valeur	
supportedAlgorithms#1	reference	1
	Algorithm	544 (SHA-1)
	parameters	NULL :NULL
	supportedOperations	Hash
	objID	1 3 14 3 2 26
	algRef	16
supportedAlgorithms#2	reference	2
	Algorithm	592 (SHA-256)
	parameters	NULL :NULL
	supportedOperations	Hash
	objID	2 16 840 1 101 3 4 2 1
	algRef	32
supportedAlgorithms#3	reference	3
	Algorithm	6 (Signature digitale avec RSA SHA-1 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 5
	algRef	18
supportedAlgorithms#4	reference	4
	Algorithm	64 (Signature digitale avec RSA SHA-256 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 11
	algRef	34

Données	Valeur	
upportedAlgorithms#5	reference	5
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 1
	algRef	2
supportedAlgorithms#6	reference	6
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	Decipher
	objID	1 2 840 113549 1 1 1
	algRef	26

Table 7-3 : EF.CIAInfo_Adèle Générique : Valorisation des éléments (2nd partie) : Liste des algorithmes supportés

Note Bene : Seuls les algorithmes utiles devront être décrits.

7.1.2 - 5031 - EF.OD

Entête :

Tag	L	Description	Valeur
62	18	*File Control Parameter (FCP)*	

Tag	L	Description	Valeur
80	02	Nombre d'octets du fichier	0x60
82	01	Descripteur de fichier	0x01 (EF transparent)
83	02	Identificateur de fichier	0x50 31
88	01	Identificateur de fichier court	0x88(SFI=11)
85	01	Niveau de renforcement	0x00
8A	01	Etat du cycle de vie	0x05
8C	03	Attribut de sécurité "compact"	0x03 17 00

DELETE FILE	Interdit
TERMINATE FILE	Interdit
ACTIVATE FILE	Interdit
DEACTIVATE FILE	Interdit
UPDATE BINARY	PIN Global
READ BINARY	Libre

Contenu :

```
-- le Path étendu n'est pas requis dans la mesure où tous les fichiers 7816-15 se trouvent sous
l'application CIA. Le chemin spécifié est alors un chemin relatif par rapport au DF sélectionné --
```

privateKeys :
```
 path :{
          efidOrPath '0x7002'
       },
```

publicKeys :
```
 path :{
          efidOrPath '0x7004'
       },
```

certificates :
```
 path :{
          efidOrPath '0x7005'
      },
```

dataContainerObjects :
```
 path :{
          efidOrPath '0x7006'
      },
```

authObjects :
```
 path :{
          efidOrPath '0x7001'
      },
```

Ce qui donne au format BER-TLV :

```
T=A0 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 02

T=A1 L=0x06
    T=30 L=0x04
        T=04 L=2
                70 04

T=A4 L=0x06
    T=30 L=0x04
        T=04 L=2
                70 05

T=A7 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 06

T=A8 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 01
```

Le contenu ci-dessus décrit est un exemple possible, il peut être modifié notamment pour l'ajout de fichiers destinés à recevoir des clès publiques.

7.1.3 - 7001 - EF.AOD

Ce fichier décrit les objets utilisés lors d'une authentification du porteur ou d'une authentification externe.
Entête :

Tag	L	Description			Valeur	
62	13	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 01	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 17 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	PIN global
					READ BINARY	Libre

Contenu :

Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PIN de la carte »
	authId	Reference au Class.authId du PUK	Obligatoire	'02'
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'C1'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PIN Global)
		change-disable[10]		*A voir avec l'émetteur*
		Unblock disable		*A voir avec l'émetteur*
		Initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Faux
		soPassword		Faux
		Disabble-allowed		Faux
		Integrity-protected		Faux
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'04'
	stroredLength	Longueur du PIN	obligatoire	'04'
	maxLength	Longueur Max du PIN	Optionnel	'04'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	01

Table 7-4 : EF.AOD_Adèle Générique : Description de l'objet PIN_Global

[10] A voir avec l'émetteur

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PUK pour PIN de la carte »
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'02'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PUK global)
		change-disable		Dépend du statut CHANGE REFERENCE DATA du PUK Global. Voir section 4.1.2 -
		Unblock disable		Vrai
		initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Vrai
		soPassword		Faux
		Disable-allowed		Faux
		Integrity-protected		Dépend du statut VERIFY (SMI ou non) du PUK Global. Voir section 4.1.2 -
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'06'
	stroredLength	Longueur du PIN	obligatoire	'06'
	maxLength	Longueur Max du PIN	Optionnel	'06'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	02

Table 7-5 : EF.AOD_Adèle Générique : Description de l'objet PUK_Global

7.1.4 - 7002 - EF.PrKD

Ce fichier contient une description des clés privées utilisées lors de services cryptographiques.

Entête :

Tag	L	Description			Valeur	
62	13	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 02	
		88	NA	Identificateur de fichier court	vide	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 17 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	PIN Global
					READ BINARY	Libre

Contenu :

Le fichier devra être dimensionné en fonction des usages prévus (nombre de clés privées).

7.1.5 - 7003 -EF.SK

L'application ne faisant pas usage de clés symétriques, ce fichier n'est pas utile et ne sera pas créé par le middleware.

7.1.6 - 7004 - Description des clés publiques (EF.PuKD)

Ce fichier sera créé si nécessaire par le middleware.

7.1.7 - 7005 - Description des certificats (EF.CD)

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 05	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 17 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	PIN Global
					READ BINARY	Libre

Contenu :
Le tableau suivant précise les données devant être renseignées dans ce fichier. La valorisation des éléments devra être réalisée en fonction des clés créées et des cas d'usage devant être supportés.

Attributs	Item	Description	Obligatoire/ Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	
	accessControlRules		obligatoire	
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
Type	Path	Chemin d'accès au certificat	obligatoire	

Table 7-6 : EF.CD_Adèle Générique : Description de l'objet Certificat

7.1.8 - 7006 - EF.DCOD

Ce fichier fournit les informations nécessaires à la gestion des objets non cryptographiques des applications utilisant les interfaces PKCS#11 et MS CAPI pour la mise à jour des données cryptographiques et non cryptographiques.

Entête :

Tag	L	Description			Valeur
62	16	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		80	02	Nombre d'octets du fichier	*A définir*
		82	01	Descripteur de fichier	0x01 (EF transparent)
		83	02	Identificateur de fichier	0x70 06
		88	01	Identificateur de fichier court	NA
		8A	01	Etat du cycle de vie	0x05
		8C	03	Attribut de sécurité « compact »	0x03 44 00

DELETE FILE	Interdit
TERMINATE FILE	Interdit
ACTIVATE FILE	Interdit
DEACTIVATE FILE	Interdit
UPDATE BINARY	Global PIN
READ BINARY	Libre

Contenu :

Pour fournir les informations, des éléments de description de type « opaqueDO » sont utilisés. Ce fichier contient des pointeurs vers d'autres fichiers contenant les données non-cryptographiques introduites par les applications. Cependant ce fichier peut-être utilisé par le CSP pour identifier le certificat par défaut à utiliser dans le cadre du Smart Card Logon (Voir annexe C).

Les tableaux ci-après décrivent la structure des éléments de données devant figurer dans le fichier ainsi que les attributs associés devant être décrits. La mise en forme au format « ISO 7816-15 » doit être faite après avoir renseigné les différents attributs.

Attributs	Item	Description	
CommonObject	Label	Voir Tableau ci-dessous	Obligatoire
	accessControlRules	Décrit les conditions d'accès au fichier	Obligatoire
Class	ApplicationName	AID de l'application adèle (??)	Obligatoire
Type	ExtendedPath	Chemin d'accès au fichier	Obligatoire

Figure 7-6 : EF.DCOD_Adèle Générique : Attributs des objets "opaqueDO"

7.2 - L'environnement de sécurité

7.2.1 - FFFB07 – SE#7 SE dédié à l'exploitation des fonctions crypto protégée sous PIN Global.

Tag	L	Description	Valeur
FFFB07	27	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 03
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*CRT Authentification PIN Global*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x08
83	01	Référence du PIN	0x01
80	01	Identifiant d'algorithme	0x00

Le SE ne référence pas de CRT d'authentification asymétrique, de déchiffrement, ou de signature car le SE courant sera construit au fur et à mesure des besoins de l'application.

7.3 - Les fichiers/objets cryptographiques de l'application

Afin de faciliter la mise à jour via PKCS#11, il est recommandé de prévoir deux clés associées à un usage. Chacune des clés étant composées de deux SDOs, un objet pour la partie privée de la clé RSA et un objet pour la partie publique. La partie publique est absolument nécessaire dès que la clé doit être générée par la carte. L'appairage entre partie privée et partie publique se fait par l'identifiant du SDO. Le tableau suivant montre cet appairage.

Les SDO seront identifiés conformément aux règles suivantes :

Identifiant SDO Privé	Identifiant SDO Public
FF9001	FFA001
FF9002	FFA002

FF9001F	FFA001F

L'appairage entre les deux clés de même usage est libre.

7.3.1 - Les fichiers « Certificat » de l'application.

Un fichier par certificat devra être créé. Le tableau suivant fourni l'entête "type" pour un tel fichier.
Entête :

Tag	L	Description			Valeur	
62	17	File Control Parameter (FCP)				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xB0 0x	
		88	NA	Identificateur de fichier court	Vide	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x7B 17 17 17 17 17 00	
					DELETE FILE	PIN Global
					TERMINATE FILE	PIN Global
					ACTIVATE FILE	PIN Global
					DEACTIVATE FILE	PIN Global
					UPDATE BINARY	PIN Global
					READ BINARY	Libre

Contenu :
Il est préconisé d'inscrire les certificats au format binaire.
Les identifiants seront créé à partir de l'identifiant générique '0xB0 01'. Le premier certificat aura pour identifiant 0xB0 01, le second 0xB002 et ainsi de suite en incrémentant l'identifiant.

7.3.2 - SDO des clés RSA

Tous les SDO nécessaires à l'application et aux usages envisagés devront être créés au moment de la personnalisation de la carte. Ci-après sont résumées les conditions d'accès à ces SDOs.

	Opérations	Clé privée	Clé publique
Avec génération de clé par la carte	PSO SIGN	Interdit	Interdit
	INTERNAL AUTHENTICATE	PIN Global ou Interdit	Interdit
	PSO DECIPHER	Interdit ou PIN Global[11]	Interdit
	GENERATE KEY PAIR	PIN Global	PIN Global
	RFU	Interdit	Interdit
	PUT DATA	interdit	interdit
	GET DATA	Libre	Libre
	Attributs de sécurité compacts	0x29 17 17 00 ou 0x19 17 17 00	0x09 17 00
Avec importation de clé	PSO SIGN	Interdit	Interdit
	INTERNAL AUTHENTICATE	PIN Global ou Interdit	Interdit
	PSO DECIPHER	Interdit ou PIN Global	Interdit
	GENERATE KEY PAIR	interdit	interdit
	RFU	Interdit	Interdit
	PUT DATA	PIN Global	PIN Global
	GET DATA	Libre	Libre
	Attributs de sécurité compacts	0x23 17 17 00 ou 0x13 17 17 00	0x03 17 00

[11] Fonction de l'usage de la clé

8 - ADF CIA Adèle Administrateur 2

Ce DF contient les fichiers 7816-15 : le fichier *EF.CIAInfo*, le fichier *EF.OD* ainsi que les autres fichiers à savoir : Le fichier *EF.AOD* et le fichier *EF.PrKD*. Le fichier EF.DCOD est facultatif. Les fichiers *EF.SKD* et *EF.PUKD* ne sont pas présents. Les deux fichiers *EF.CIAInfo* et *EF.OD* n'ont pas besoin d'être mis à jour. Les autres fichiers descripteurs conformes à la norme 7816-15 peuvent être mis à jour et bénéficient ainsi des environnements de sécurité de cette application.

Tag	L	Description			Valeur	
62	17	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		82	01	Descripteur de fichier	0x38 (répertoire)	
		84	0F	Nom de l'ADF (AID)	0xE8 28 BD 08 0F A compléter	
		8C	01	Attribut de sécurité "compact"	0x00	
					DELETE FILE (sur le DF lui-même)	Interdit
					TERMINATE FILE	SMI PSCe2
					ACTIVATE FILE	SMI PSCe2
					DEACTIVATE FILE	SMI PSCe2
					CREATE FILE (DF)	SMI PSCe2
					CREATE FILE (EF) / PUT DATA (SDO)	SMI PSCe2

8.1 - Les fichiers 7816-15

8.1.1 - 5032 - EF.CIAInfo

Entête :

Tag	L	Description			Valeur	
62	15	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x50 32	
		88	01	Identificateur de fichier court	0x90 (SFI=12)	
		8A	01	Etat du cycle de vie	*A définir*	
		8C	02	Attribut de sécurité "compact"	0x0100	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	Interdit
					READ BINARY	libre

Contenu :
Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Données	Description		Obligatoire/ Optionnel
Version	Identifie la version de spécification ISO7816-15		Obligatoire
serialNumber	Identifiant unique de la carte. Cette donnée doit être présente si l'information est considérée comme non confidentielle (i.e. en lecture libre) sinon elle doit être omise		optionnel
Label	Contient des données d'identification de l'application pouvant être affichées par une application « terminal »		optionnel
Cardflags	Donne des informations sur la carte :		Obligatoire
	readonly	Si la carte est en lecture seule	
	authRequired	Si des fonctions crypto. requièrent l'authentification du porteur	
	prnGeneration	Si la carte supporte la génération de quantité pseudo-aléatoire	
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l'application. Est composé des sous champs suivants :		Optionnel
	se	Désigne le numéro de SE	Obligatoire
	Owner	Dans le présent contexte désignera le propriétaire du jeu de clé pointé par le se	
	Aid	AID de l'application contenant le SE	
supportedAlgorithms	Décrit les différents algorithmes supportés par la carte ainsi que ses paramètres. Comprend les sous champs suivants :		
	reference	Identifiant unique dans l'application CIA	Obligatoire
	Algorithm	Identifiant d'algorithm selon PKCS#11	
	parameters	Paramètres d'utilisation de l'algorithme	
	supportedOperations	Liste des opérations pouvant être réalisées avec cet algorithme	
	objID	Identifiant type 'OID'	
	algRef	Identifiant de l'algorithme tel que géré par l'application IAS associée.	

Table 8-1 : EF.CIAInfo_Adèle Administrateur 2 : Description du contenu

Données	Valeur	
Version	2	
serialNumber	--	
Label	'A compléter'	
Cardflags	Donne des informations sur la carte :	
	readonly	Oui
	authRequired	Oui
	prnGeneration	Oui
seInfo	Énumère les environnements de sécurité SE auxquels fait appel l'application.	
	se	2, 4, 7
	Owner	Pour les se #2: OID PSCe2 (administrateur de l'application) Pour le se #7 : non renseigné
	Aid	Pour tous les se AID de l'application Adèle Administrateur 2 (i.e. A compléter)
supportedAlgorithms	Voir tableau suivant	

Table 8-2 : EF.CIAInfo_Adèle Administrateur 2 : Valorisation des éléments (1ere partie)

Données	Valeur	
supportedAlgorithms#1	reference	1
	Algorithm	544 (SHA-1)
	parameters	NULL :NULL
	supportedOperations	Hash
	objID	1 3 14 3 2 26
	algRef	16
supportedAlgorithms#2	reference	2
	Algorithm	592 (SHA-256)
	parameters	NULL :NULL
	supportedOperations	Hash
	objID	2 16 840 1 101 3 4 2 1
	algRef	32
supportedAlgorithms#3	reference	3
	Algorithm	6 (Signature digitale avec RSA SHA-1 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 5
	algRef	18
supportedAlgorithms#4	reference	4
	Algorithm	64 (Signature digitale avec RSA SHA-256 format PKCS#1)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 11
	algRef	34
upportedAlgorithms#5	reference	5
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	Compute signature
	objID	1 2 840 113549 1 1 1
	algRef	2
supportedAlgorithms#6	reference	6
	Algorithm	1 (RSA format PKCS#1 sans digest info)
	parameters	NULL :NULL
	supportedOperations	Decipher
	objID	1 2 840 113549 1 1 1
	algRef	26

Table 8-3 : EF.CIAInfo_Adèle Administrateur 2 : Valorisation des éléments (2ere partie) : Liste des algorithmes supportés

```
-- EF.CIAInfo
adele-1-EFCIAInfo CIAInfo ::= SEQUENCE
{  version v2, -- version de ISO/IEC 7816-15
       label "Adèle", -- peut contenir aussi manufacturerID[12]
       cardflags { authRequired, prnGeneration },
       seInfo
       { { se 2,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid A compléter'H }, -- AID Adèle Administrateur 2
         { se 4,
       owner object identifier identifiant le propriétaire du jeu de clé associé au SE
       aid 'A compléter'H },
         { se 7,
       aid 'A compléter'H },
       },
supportedAlgorithms
{
-- AlgID: 0x10, SHA-1
    { reference 1, -- unique référence dans CIA
    algorithm 544, -- calcul de condensat ref.PKCS#1,conforme ECC-2
    parameters NULL: NULL, -- type de paramètre NULL et valeur NULL
    supportedOperations {hash},
    objId {1 3 14 3 2 26},
    algRef 16 -- equivalent 0x10, algoID dans appli Adle, IAS V1.0
    },

-- Hash algorithm
-- AlgID: 0x40, SHA-256
    { reference 2, -- unique rfrence dans CIA
    algorithm 592, -- calcul de condens ref.PKCS#1,conforme ECC-2
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {hash},
    objId {2 16 840 1 101 3 4 2 1},
    algRef 32 -- equivalent 0x20, algoID IAS V1.0 Note that this is different from ECC-2
    },

-- Signature algorithm
-- Signature numrique RSA selon PKCS#1 avec SHA-1
    { reference 3, -- unique reference CIA, rfrence croise avec EF.PrKD
    algorithm 6, -- mcanisme RSA PKCS#1 avec SHA-1 = 0x12
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {compute-signature},
    objId {1 2 840 113549 1 1 5},
    algRef 18 -- equivalent 0x12, algoID dans appli Adle, IAS V1.0
},

-- Signature algorithm
-- Signature numrique RSA selon PKCS#1 avec SHA-256
    { reference 4, -- unique reference CIA, rfrence croise avec EF.PrKD
    algorithm 64, -- mcanisme RSA PKCS#1 avec SHA-256 = 0x22
    parameters NULL: NULL, -- type de parametre NULL et valeur NULL
    supportedOperations {compute-signature},
    objId {1 2 840 113549 1 1 11},
    algRef 34 -- equivalent 0x22, algoID dans appli Adle, IAS V1.0
},


-- C/S algorithm
-- Authentification Client/Serveur, signature RSA selon PKCS#1 sans info
-- abrges
-- AlgID: 0x02, C/S AUT
{ reference 5, -- unique reference CIA, rfrence croise avec EF.PrKD
        algorithm 1, -- mcanisme RSA PKCS#1 sans digest info = 0x02
        parameters NULL: NULL, -- type de parametre NULL et valeur NULL
        supportedOperations {compute-signature},
```

[12] Le numéro de serie est géré via le fichier EF.DCOD. Le 'ManufacturerID' est optionnel mais pas vraiment utile dans le cadre de l'utilisation. Les problèmes doivent être remonter vers l'émetteur qui est identifié par l'EF.DIR.

```
        objId {1 2 840 113549 1 1 1}, -- RSA with PKCS #1 padding
        algRef 2 -- equivalent 0x02, algoID dans appli Adle, IAS V1.0
},

-- Key decipherment algorithm
-- Key decipherment using RSA with PKCS #1 padding
-- AlgID: 0x02, C/S AUT
{ reference 6, -- unique reference CIA, rfrence croise avec EF.PrKD
        algorithm 1, -- mcanisme RSA PKCS#1 = 0x1A
        parameters NULL: NULL, -- type de parametre NULL et valeur NULL
        supportedOperations {decipher},
        objId {1 2 840 113549 1 1 1}, --  RSA with PKCS #1 padding
        algRef 26 -- equivalent 0x1A, algoID dans appli Adle, IAS V1.0
},
}}
```

8.1.2 - 5031 - EF.OD

Entête :

Tag	L	Description			
62	18	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		80	02	Nombre d'octets du fichier	0x60
		82	01	Descripteur de fichier	0x01 (EF transparent)
		83	02	Identificateur de fichier	0x50 31
		88	01	Identificateur de fichier court	0x88(SFI=11)
		85	01	Niveau de renforcement	0x00
		8A	01	Etat du cycle de vie	0x05
		8C	02	Attribut de sécurité "compact"	0x01 00 DELETE FILE — Interdit TERMINATE FILE — Interdit ACTIVATE FILE — Interdit DEACTIVATE FILE — Interdit UPDATE BINARY — Interdit READ BINARY — Libre

Contenu :

```
-- le Path étendu n'est pas requis dans la mesure où tous les fichiers 7816-15 se trouvent sous
l'application CIA. Le chemin spécifié est alors un chemin relatif par rapport au DF sélectionné --
```

privateKeys :

```
 path :{
          efidOrPath '0x7002'
        },
```

```
Ce qui donne au format BER-TLV :

T=A0 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 02
```

certificates :

```
 path :{
          efidOrPath '0x7005'
      },
```

```
T=A4 L=0x06
    T=30 L=0x04
        T=04 L=2
                70 05
```

dataContainerObjects :

```
 path :{
          efidOrPath '0x7006'
      },
```

```
T=A7 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 06
```

authObjects :

```
 path :{
          efidOrPath '0x7001'
      },
```

```
T=A8 L=0x06
    T=30 L=0x04
        T=04 L=02
                70 01
```

8.1.3 - 7001 - EF.AOD

Ce fichier décrit les objets utilisés lors d'une authentification du porteur ou d'une authentification externe.
Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 01	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe2
					READ BINARY	Libre

Contenu :

Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PIN de la carte »
	authId	Reference au Class.authId du PUK	Obligatoire	'02'
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'C1'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PIN Global)
		change-disable[13]		*A voir avec l'émetteur*
		Unblock disable		*A voir avec l'émetteur*
		Initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Faux
		soPassword		Faux
		Disabble-allowed		Faux
		Integrity-protected		Faux
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'04'
	stroredLength	Longueur du PIN	obligatoire	'04'
	maxLength	Longueur Max du PIN	Optionnel	'04'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	01

Table 8-4 : EF.AOD_Adèle Administrateur 2 : Description de l'objet PIN_Global

[13] A voir avec l'émetteur

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	« PUK pour PIN de la carte »
	accesControlRules		Optionnel	Non renseigné
Class	authId	Identifiant	Obligatoire	'02'
Type	pwdFlags	case-sensitive	obligatoire	Faux (PIN numérique)
		Local		Faux (PUK global)
		change-disable		Dépend du statut CHANGE REFERENCE DATA du PUK Global. Voir section 4.1.2 -
		Unblock disable		Vrai
		initialized		Vrai : Le PIN est initialisé
		Needs-padding		Faux (pas de padding)
		unblockingPassword		Vrai
		soPassword		Faux
		Disable-allowed		Faux
		Integrity-protected		Dépends du statut VERIFY (SMI ou non) du PUK Global. Voir section 4.1.2 -
		Confidentiallity-protected		Faux
		exchangeRefData		0
	PwdType	Type de codage	obligatoire	Ascii-Numérique
	minLength	Longueur Min du PIN	obligatoire	'06'
	stroredLength	Longueur du PIN	obligatoire	'06'
	maxLength	Longueur Max du PIN	Optionnel	'06'
	pwdReference	Référence à utiliser dans la commande Verify	obligatoire	02

Table 8-5 : EF EF.AOD_Adèle Administrateur 2 : Description de l'objet PUK_Global

8.1.4 - 7002 - EF.PrKD

Ce fichier contient une description des clés privées utilisées lors de services cryptographiques.

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 02	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe
					READ BINARY	Libre

Contenu :

Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé d'authentification »**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		Modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide (correspond à pas de compteur)
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	Encipher	Obligatoire	non
		Decipher		non
		Sign		Oui
		signRecover		non
		keyEncipher		non
		Verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		non
	accessFlags	Sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'01'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	'01' RSA format PKCS#1 sans digestInfo
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 8-6 : EF.PrKD_Adèle Administrateur 2 : Description de l'objet Clé RSA d'authentification

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé de signature»**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		Modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	Encipher	Obligatoire	non
		Decipher		non
		Sign		Oui
		signRecover		non
		keyEncipher		non
		Verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		**Doit être cohérent avec le flag « NonRépudiation » contenu dans le tag '9E' du SDO de la clé associée**
	accessFlags	Sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'02'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	'06' si DSI avec RSA et SHA-1 '64' si DSI avec RSA et SHA-256
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 8-7 : EF.PrKD_Adèle Administrateur 2 : Description de l'objet Clé RSA de signature

Attributs	Item	Description	Obligatoire/Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**« Clé de déchiffrement de clé»**
	Flags	Private	Obligatoire	Vrai (verification du porteur requise avant utilisation)
		Modifiable		**Faux** (pour support PKCS#11)
	userConsent		Conditionnel	Vide (pas de reset du PIN après utilisation)
	accessControlRules		obligatoire	Voir tableau accesControlRules ci dessous
Class	iD	Identifiant Unique	obligatoire	**Voir règle de génération des Id uniques**
	Usage	Encipher	Obligatoire	non
		Decipher		non
		Sign		non
		signRecover		non
		keyEncipher		non
		keyDecipher		oui
		Verify		non
		verifyRecover		non
		derive		non
		nonRepudiation		non
	accessFlags	Sensitive	Obligatoire	Vrai (clé privée)
		Extractable		Faux (non recouvrable depuis la carte)
		AlwaysSensitive		Vrai
		NeverExtractable		Vrai
		CardGenerated		Vrai si la clé est générée par la carte Faux sinon
	keyReference	Référence utilisée dans le CRT	obligatoire	'03'
	algReference	Liste des références des algorithmes supportées pour la clé	obligatoire	'01' RSA format PKCS#1 sans digestInfo
Type	Path	Chemin d'accès au SDO	obligatoire	Vide (empty)
	Modulus length	Longueur du modulo en bits	obligatoire	

Table 8-8 : EF.PrKD_Adèle Administrateur 2 : Description de l'objet Clé RSA de déchiffrement

AccessMode		Security Condition		
Field	Operation	Clé d'authentification	Clé de signature	Clé de déchiffrement
Read	-			
Update	Update or Generate Key Pair	NA [14]	NA	NA
Execute	InternalAuth, PSOCompute, PSODecipher	'C1'	'C1'	'C1'
Delete	-			

Table 8-9 : EF.PrKD_Adèle Administrateur 2 : accessControlRules pour les clés RSA

[14] voir Flag « modifiable »

8.1.5 - 7005 - Description des certificats (EF.CD) (P)

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 05	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe2
					READ BINARY	Libre

Contenu :
Les tableaux suivants précisent les données devant être renseignées dans ce fichier.

Attributs	Item	Description	Obligatoire/ Optionnel	Value
Common	Label	Label décrivant l'objet	Obligatoire	**Voir Tableau ci-dessous**
	accessControlRules		obligatoire	
Class	iD	Identifiant Unique		**Voir Tableau ci-dessous**
Type	Path	Chemin d'accès au certificat		**Voir Tableau ci-dessous**

Table 8-10 : EF.CD_Adèle Administrateur 2 : Description de l'objet Certificat

Label	iD	path[15]
« Certificat d'authentification »	'01'	'A001'
« Certificat de signature »	'02'	'A002'
« Certificat de déchiffrement de clé»	'03'	'A003'

Table 8-11 : EF.CD_Adèle Administrateur 2 : Liste des certificats (non CA) devant apparaître dans EF.CD

AccessMode		Security Condition
Field	Operation	
Read	Read	always
Update	Update	authReference { authMethod=secureMessaging seIdentifier=4}
Execute	-	
Delete	-	

Table 8-12 : EF.CD_Adèle Administrateur 2 : accessControlRules pour les certificats

[15] La référence est relative par rapport au DF courant

8.1.6 - 7006 - EF.DCOD

La présence de ce fichier est conditionnelle : Il doit être présent si l'application requière de référencer un objet non crypto non déjà décrit dans une autre application CIA de la carte.

Entête :

Tag	L	Description			Valeur	
62	16	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0x70 06	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	03	Attribut de sécurité "compact"	0x03 44 00	
					DELETE FILE	Interdit
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe2
					READ BINARY	Libre

Contenu :

Pour fournir les informations, des éléments de description de type « opaqueDO » sont utilisés

Les tableaux ci-après décrivent les éléments de données devant figurer dans le fichier ainsi que les attributs associés devant être décrits. La mise en forme au format « ISO 7816-15 » doit être faite après avoir renseigné les différents attributs.

Attributs	Item	Description	
CommonObject	Label	Voir Tableau ci-dessous	Obligatoire
	accessControlRules	Décrit les conditions d'accès au fichier	Obligatoire
Class	ApplicationName	AID de l'application adèle (??)	Obligatoire
Type	ExtendedPath	Chemin d'accès au fichier	Obligatoire

Table 8-13 : EF.DCOD_Adèle Administrateur 2 : Attributs des objets "opaqueDO"

8.2 - Les fichiers/objets d'administration de l'application

Les fichiers ou objets d'administration sont décrits dans ce paragraphe. Les différents objets décrits sont :

Les environnements de sécurité. Ils sont au nombre de trois :

- Le SE#2 dédié à la gestion administrative de l'application quand les protections font appel à l'authentification mutuelle, l'intégrité, la confidentialité. Les clés correspondantes sont sous contrôle d'un PSCe2 (PSCe2_KeySet).

- Le SE#4 dédié à la gestion administrative de l'application quand les protections font appel à l'authentification mutuelle, l'intégrité et/ou du porteur par PIN Global. Les clés correspondantes sont sous contrôle d'un PSCe2 (PSCe2_KeySet).

- Le SE#7 dédié à la gestion des protections des fonctions cryptographiques mises en œuvre par l'application (hors administration). Cet environnement ne référence que le PIN_Global.

8.2.1 - FFFB02 – SE#2 dédié à la gestion administrative de l'application par PSCe2

Ce SE doit être utilisé pour une protection en Secure Messaging faisant appel à une authentification mutuelle, de l'intégrité et de la confidentialité.

Tag	L	Description	Valeur
FFFB02	3D	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 03
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*Authentification Mutuelle symétrique PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x C0
83	01	Référence du jeu de clés symétriques d'authentification	0x 82 (PSCe2)
80	01	Identifiant d'algorithme	0x 1C

Tag	L	Description	Valeur
B4	09	*CRT de SMI PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82
80	01	Identifiant d'algorithme	0x1C

Tag	L	Description	Valeur
B8	09	*CRT de SMC PSCe2*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82
80	01	Identifiant d'algorithme	0x1C

8.2.2 - FFFB04 - SE#4 dédié à la gestion administrative de la carte par un PSCe2 – Intégrité Uniquement

Ce SE doit être utilisé pour des besoins de protection en intégrité seule.

Tag	L	Description	Valeur
FFFB02	32	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	0x00 02
84	10	Nom de l'objet de sécurité	
8C	02	Attribut de sécurité "compact"	0x81 00

RFU	Interdit
RFU	Interdit
RFU	Interdit
RFU	Interdit
MANAGE SE	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
A4	09	*Authentification Mutuelle symétrique*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x C0
83	01	Référence du jeu de clés symétriques d'authentification	0x 82 (PSCe2)
80	01	Identifiant d'algorithme	0x 1C

Tag	L	Description	Valeur
B4	09	*CRT de SMI PSCe*	

Tag	L	Description	Valeur
95	01	Octet d'usage (UQB)	0x30
83	01	Référence du jeu de clés symétriques d'authentification	0x82
80	01	Identifiant d'algorithme	0x1C

8.2.3 - FFFB07 – SE#7 SE dédié à l'exploitation des fonctions crypto protégée sous PIN Global.

Ce SE doit être utilisé pour les clés d'authentification et de chiffrement pour les profils *, ** ou *** ; et pour les clés de signature dans le cas de profils * ou **.

Tag	L	Description	Valeur
FFFB07	27	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1A	*DOCP*	

Tag	L	Description	Valeur

		80	02	Longueur du DOUP	0x00 01	
		84	10	Nom de l'objet de sécurité		
		8C	02	Attribut de sécurité "compact"	0x81 00	
					RFU	Interdit
					RFU	Interdit
					RFU	Interdit
					RFU	Interdit
					MANAGE SE	Interdit
					PUT DATA	Interdit
					GET DATA	Libre
	Tag	**L**	**Description**		**Valeur**	
	A4	09	*CRT Authentification PIN Global*			
			Tag	**L**	**Description**	**Valeur**
			95	01	Octet d'usage (UQB)	0x08
			83	01	Référence du PIN	0x01
			80	01	Identifiant d'algorithme	0x00

Le SE ne référence pas de CRT d'authentification asymétrique, de déchiffrement, ou de signature car le SE courant sera construit au fur et à mesure des besoins de l'application.

8.2.4 - –FF8A02 – Jeu de Clés symétriques PSCe2

Tag	L	Description	Valeur
FF8A02	51	*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	2	Longueur du DOUP	0x00 10
84	10	Nom de l'objet de sécurité	*Hérité des paramètres de la clé mère*
8C	3	Attribut de sécurité "compact"	0x89 00 00

RFU	Interdit
EXTERNAL AUTHENTICATE	Interdit
RFU	Interdit
MUTUAL AUTHENTICATE	Libre
RFU	Interdit
PUT DATA	Interdit
GET DATA	Libre

Tag	L	Description	Valeur
9A	1	Nombre maximum d'erreurs autorisé	*Hérité des paramètres de la clé mère*
9B	1	Compteur d'erreurs	*Hérité des paramètres de la clé mère*
9C	2	Compteur d'utilisations	*Hérité des paramètres de la clé mère*
7F4B	27	*Valeur des clés*	

Tag	L	Description	Valeur
90	10	K MAC	*Dérivée de la clé mère*
91	10	K ENC	*Dérivée de la clé mère*
80	1	Algorithme d'usage	*Hérité des paramètres de la clé mère*

8.3 - Les fichiers/objet cryptographiques de l'application

Dans cette implémentation, il a été choisi de supporter un fichier par type de certificat.

8.3.1 - A001 - Certificat d'authentification Carte

Entête :

Tag	L	Description			Valeur
62	1D	*File Control Parameter (FCP)*			
		Tag	**L**	**Description**	**Valeur**
		80	02	Nombre d'octets du fichier	*A définir*
		82	01	Descripteur de fichier	0x01 (EF transparent)
		83	02	Identificateur de fichier	0xA0 01
		88	01	Identificateur de fichier court	NA
		8A	01	Etat du cycle de vie	0x05
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00 DELETE FILE — SMI PSCe2 TERMINATE FILE — Interdit ACTIVATE FILE — Interdit DEACTIVATE FILE — Interdit UPDATE BINARY — SMI PSCe2 READ BINARY — Libre

Contenu :
Il est préconisé d'inscrire le certificat au format binaire.

8.3.2 - A002 - Certificat de signature porteur

Entête :

Tag	L	Description			Valeur	
62	1D	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xA0 02	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00	
					DELETE FILE	SMI PSCe2
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe 2
					READ BINARY	Libre

Contenu :
Il est préconisé d'inscrire le certificat au format binaire.

8.3.3 - A003 - Certificat de chiffrement

Entête :

Tag	L	Description			Valeur	
62	1D	*File Control Parameter (FCP)*				
		Tag	**L**	**Description**	**Valeur**	
		80	02	Nombre d'octets du fichier	*A définir*	
		82	01	Descripteur de fichier	0x01 (EF transparent)	
		83	02	Identificateur de fichier	0xA0 03	
		88	01	Identificateur de fichier court	NA	
		8A	01	Etat du cycle de vie	0x05	
		8C	07	Attribut de sécurité "compact"	0x43 44 44 00	
					DELETE FILE	SMI PSCe2
					TERMINATE FILE	Interdit
					ACTIVATE FILE	Interdit
					DEACTIVATE FILE	Interdit
					UPDATE BINARY	SMI PSCe2
					READ BINARY	Libre

Contenu :
Il est préconisé d'inscrire le certificat au format binaire.

8.3.4 - FF9001 – Clé Privée dédiée à l'authentification (sans génération par la carte)

Tag	L	Description	Valeur
FF9001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA3 17 C2 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	PIN Global
PSO DECIPHER	Interdit
GENERATE KEY PAIR	interdit
RFU	Interdit
PUT DATA	SMIC PSCe
GET DATA	Libre

9C	2	Compteur d'utilisations	0xFF FF[8]
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction d'authentification est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe2 en introduisant la valeur de la clé par par un canal sécurisé en confidentialité.

[8] Le compteur d'utilisation est positionné à la valeur maximale, mais peut être mis à une autre valeur en fonction de l'application
[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.5 - FF9001 – Clé Privée dédiée à l'authentification (avec génération par la carte)

Tag	L	Description	Valeur
FF9001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA9 17 C4 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	PIN Global
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe2
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
9C	2	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction d'authentification est protégée par authentification du porteur sous PIN global. La génération de la valeur de la clé se fait sous contrôle du PSCe. La commande *GenerateKeyPair* doit être protégée en intégrité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.6 - FF9002 – Clé Privée dédiée à la signature (sans génération de clé par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA2 17 C2 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	PIN Global
PSO DECIPHER	Interdit
GENERATE KEY PAIR	interdit
RFU	Interdit
PUT DATA	SMIC PSCe2
GET DATA	Libre

Tag	L	Description	Valeur
9C	2	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction de signature est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe2 en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.7 - FF9002 – Clé Privée dédiée à la signature (avec génération de clé par la carte)

Tag	L	Description	Valeur
FF9002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0xA2 17 C2 00 PSO SIGN : Interdit INTERNAL AUTHENTICATE : PIN Global PSO DECIPHER : Interdit GENERATE KEY PAIR : SMIC PSCe2 RFU : Interdit PUT DATA : Interdit GET DATA : Libre

Tag	L	Description	Valeur
9C	2	Compteur d'utilisations	0xFF FF
7F48	028D[9]	*Valeur de la clé privée*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x02

La fonction de signature est protégée par authentification du porteur sous PIN global. La génération de la valeur de la clé se fait sous contrôle du PSCe. La commande *GenerateKeyPair* doit être protégée en intégrité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.8 - FF9003 – Clé Privée de Chiffrement (sans génération de clé par la carte)

Tag	L	Description	Valeur
FF9003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0x93 17 C2 00

PSO SIGN	Interdit
INTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	PIN Global
GENERATE KEY PAIR	Interdit
RFU	Interdit
PUT DATA	SMIC PSCe2
GET DATA	Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Non
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de chiffrement est protégée par authentification du porteur sous PIN global. L'introduction de la valeur de la clé se fait sous contrôle du PSCe en introduisant la valeur de la clé par un canal sécurisé en confidentialité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.9 - FF9003 – Clé Privée de Chiffrement (avec génération de clé par la carte)

Tag	L	Description	Valeur
FF9003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1C	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	04	Attribut de sécurité "compact"	0x99 17 C4 00 PSO SIGN — Interdit INTERNAL AUTHENTICATE — Interdit PSO DECIPHER — PIN Global GENERATE KEY PAIR — SMI PSCe2 RFU — Interdit PUT DATA — Interdit GET DATA — Libre

Tag	L	Description	Valeur
9C	02	Compteur d'utilisations	0xFF FF
9E	01	Ré-initialisation de code PIN de signature	Oui
7F48	028D[9]	*Valeur des clés*	

Tag	L	Description	Valeur
92	80[9]	p	*Non renseigné en perso*
93	80	q	*Non renseigné en perso*
94	80	q^{-1} mod p	*Non renseigné en perso*
95	80	dp	*Non renseigné en perso*
96	80	dq	*Non renseigné en perso*
80	01	Algorithme d'usage	0x12

La fonction de chiffrement est protégée par authentification du porteur sous PIN global. La génération de la valeur de la clé se fait sous contrôle du PSCe. La commande *GenerateKeyPair* doit être protégée en intégrité.

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.10 - FFA001 – Clé publique d'authentification

La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA001		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	03	Attribut de sécurité "compact"	0x89 C4 00

PSO SIGN	Interdit
EXTERNAL AUTHENTICATE	Interdit
PSO DECIPHER	Interdit
GENERATE KEY PAIR	SMI PSCe2
RFU	Interdit
PUT DATA	interdit
GET DATA	Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.11 - FFA002 – Clé publique de signature

La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA002		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	03	Attribut de sécurité "compact"	0x89 C4 00 PSO SIGN : Interdit EXTERNAL AUTHENTICATE : Interdit PSO DECIPHER : Interdit GENERATE KEY PAIR : SMI PSCe2 RFU : Interdit PUT DATA : interdit GET DATA : Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

8.3.12 - FFA003 – Clé publique de chiffrement

La présence de ce SDO n'est obligatoire que dans le cas où la clé privée correspondante doit être générée par la carte et ce afin de pouvoir retrouver le modulo.

Tag	L	Description	Valeur
FFA003		*Référence de l'objet*	

Tag	L	Description	Valeur
E2	1B	*DOCP*	

Tag	L	Description	Valeur
80	02	Longueur du DOUP	<Spécifie la taille du modulo> [9] Ex : 0x0100 pour une clé de 2048 bits (256 octets)
84	10	Nom de l'objet de sécurité	*A définir*
8C	03	Attribut de sécurité "compact"	0x89 C4 00 PSO SIGN : Interdit EXTERNAL AUTHENTICATE : Interdit PSO DECIPHER : Interdit GENERATE KEY PAIR : SMI PSCe2 RFU : Interdit PUT DATA : interdit GET DATA : Libre

Tag	L	Description	Valeur
7F49		*Valeur de la clé publique*	

Tag	L	Description	Valeur
81	0x0100[9]	Modulo	
82	04	Exposant public e	
5F4C	??	Autorisation du porteur de certificat	*A définir*

[9] A définir en fonction de la taille de la clé. Voir 12 -Annexe D : **Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.**

9 - Annexe A : Règle de génération des identifiants uniques pour les clés RSA privées et les certificats

Afin de garantir l'unicité d'un identifiant d'un objet crypto dans une carte, l'identifiant est composé comme suit :

- Les octets de poids fort sont composés de l'AID de l'application hôte.
- Un octet caractérisant le type de l'objet. Par exemple, '01' pour une clé privée RSA ou son certificat associé. Autre valeur réservé pour un usage futur.
- Un octet identifiant un objet pour une application et un type donné.

Exemple ID de la clé de signature de l'application Adèle :

<D2 50 00 00 04 41 64 E8 6C 65 01 01> <01> <02>

10 - Annexe B : Champs obligatoires et champs optionnels du profil de personnalisation

10.1 - Introduction

Dans cette annexe sont décrits les champs du profil de perso qui sont obligatoires pour que la carte IAS personnalisée soit fonctionnellement compatible avec le middleware Carte IAS.

10.2 - Applications

Un profil de perso peut comporter une ou plusieurs applications crypto, en plus de l'application émetteur.
Pour être fonctionnellement compatible avec le middleware Carte IAS, une application cryptographique doit posséder un AID commençant par 0xE8 28 BD 08 0F D2 50. Les applications décrites dans ce document sont compatibles avec cette exigence.

Applications	Voir §	Obligatoire /optionnel	Commentaire
Adèle (-Administrateur 1)	5 - et 6 -	1 Obligatoire, la 2nd Optionnelle	Au moins une de ces 2 applications doit être présente.
Adèle Générique	7 -		
Adèle -Administrateur 2	8 -	Optionnelle	
Root directory	4 -	Obligatoire	

10.3 - Root directory

Certains champs sous « le root directory » sont obligatoires pour un fonctionnement correct avec le MW-IAS de la DGME à des fins de compatibilité avec les normes ISO et d'interopérabilité.

Root directory	Voir §	Obligatoire /optionnel	Commentaire
EF_DIR	4.1.1 -	Obligatoire	
PIN Global	4.1.2 -	Obligatoire	Doit être sous le contrôle de l'émetteur
EF.ID	4.1.3 -	Obligatoire	
EF.AD	4.1.4 -	Obligatoire	
Clés Sym autorité admin	4.1.5 -	Conditionnel	Obligatoire si EF.ID et/ou EF.AD

10.4 - Contenu des applications

Dans le cas où une application crypto est présente dans la carte, certains champs sont obligatoires pour un fonctionnement correct avec le MW-IAS de la DGME, d'autres sont optionnels.

Application Adèle	Voir §	Obligatoire /optionnel	Commentaire
ADF CIA Adèle	5 -	Obligatoire	
EF.CIAInfo	5.1.1 -	Obligatoire	
EF.OD	5.1.2 -	Obligatoire	
ADF Adèle	6 -	Obligatoire	
PIN de signature	6.1.1 -	Conditionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
Unblock PIN #1	6.1.2 -	Conditionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
Unblock PIN #2	6.1.3 -	Conditionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
Unblock PIN #3	6.1.4 -	Conditionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
EF Serial nb	6.2.1 -	Obligatoire	
SE#2	6.2.2 -	Obligatoire	
SE#4	6.2.3 -	Obligatoire	
SE#7	6.2.4 -	Obligatoire	
SE#8	6.2.5 -	Optionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
SE#9	0	Optionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
Clés sym PSCe	6.2.7 -	Obligatoire	
Clés sym signature qualifiée	6.2.8 -	Conditionnel	Obligatoire si un certificat PRIS v2 *** de signature est présent
EF.AOD	6.3.1 -	Obligatoire	
EF.PrKD	6.3.2 -	Obligatoire	
EF.SK	6.3.3 -	-	Non applicable
EF.PuKD	6.3.4 -	-	Non applicable
EF.CD	6.3.5 -	Obligatoire	
EF.DCOD	6.3.6 -	Obligatoire	
EF certificat	6.4.1 -, 6.4.2 -, 6.4.3 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application
Clé privée	6.4.4 -à 6.4.11 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application
Clé publique	0 à 6.4.13 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application, si la bi-clé correspondante doit pourvoir être générée par la carte elle-même

Application : Adèle Générique	Voir §	Obligatoire /optionnel	Commentaire
ADF CIA Adèle Générique	7 -	Obligatoire	
EF.CIAInfo	7.1.1 -	Obligatoire	
EF.OD	7.1.2 -	Obligatoire	
SE#7	7.2.1 -	Obligatoire	
EF.AOD	7.1.3 -	Obligatoire	
EF.PrKD	7.1.4 -	Obligatoire	
EF.SK	7.1.5 -	-	Non applicable
EF.PuKD	7.1.6 -	Obligatoire	
EF.CD	7.1.7 -	Obligatoire	
EF.DCOD		Obligatoire	Nécessaire pour le stockage d'objet P#11 non crypto.
EF certificat	7.3.1 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application Il peut être utile de dupliquer cet élément afin de faciliter le renouvellement de certificat.
Clé privée	7.3.2 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application. Il peut être utile de dupliquer cet élément afin de faciliter le renouvellement de certificat.
Clé publique	7.3.2 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application. Il peut être utile de dupliquer cet élément afin de faciliter le renouvellement de certificat.

Application : Adèle -Administrateur 2	Voir §	Obligatoire /optionnel	Commentaire
ADF CIA Adèle Admin 2	8 -	Obligatoire	
EF.CIAInfo	8.1.1 -	Obligatoire	
EF.OD	8.1.2 -	Obligatoire	
SE#2	8.2.1 -	Obligatoire	
SE#4	8.2.2 -	Obligatoire	
SE#7	8.2.3 -	Obligatoire	
Clés sym PSCe 2	8.2.4 -	Obligatoire	
EF.AOD	8.1.3 -	Obligatoire	
EF.PrKD	8.1.4 -	Obligatoire	
EF.CD	8.1.5 -	Obligatoire	
EF.DCOD	8.1.6 -	Obligatoire	
EF certificat	8.3.1 - à 8.3.3 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application
Clé privée	8.3.4 - à 8.3.9 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application
Clé publique	8.3.10 - à 8.3.12 -	Optionnel	Obligatoire pour chaque certificat présent dans l'application, si la bi-clé correspondante doit pourvoir être générée par la carte elle-même

11 - Annexe C : Recommandation sur la taille des fichiers de l'application « GénériqueCrypto »

Cette annexe fournit des éléments afin de calculer la taille des fichiers suivants :

- EF.CD (fichier descripteur des certificats)
- EF.PrKD (fichier descripteur des clés privées)
- EF.PuKD (fichier descripteur des clés publiques)
- Et EF.DCOD ((fichier descripteur des objets non-cryptographiques)

Bien que contenant généralement des descriptions d'objets non-cryptographiques, le fichier EF.DCOD est utilisé par le CSP pour définir le certificat par défaut pour le « Smart Card Logon ». Les objets sont créés par le CSP durant l'enregistrement ou l'import d'une clé. Un objet est créé par certificat contenu dans la **carte** quelle que soit l'application.

La taille de l'objet créé est variable et dépend de l'autorité de certification. Avant de personnaliser la carte il est recommandé de vérifier l'exactitude des valeurs des paramètres ci-dessous auprès de son autorité de certification.

Paramètres de calculs	**Taille (en octets)**
Objet Label	x=40
Objet ID	y=36
Partie « Subject » du certificat[16]	z=300

Fichier	**Taille recommandée**[17]
EF.CD	$N^{18}*(60+x+y)*1,2$
EF.PrKD	$N*(85+x+y+z)*1,2$
EF.PuKD	$N*(80+x+y)*1,2$
EF.DCOD	$(N^{19}_{Total}*(68+36)+89)*1,2$

[16] La partie « subject » du certificat est optionnelle. Sa présence est décidée par le service d'enregistrement. Cette information n'est pas nécessaire dans le cas de l'application Adèle.
[17] La taille ne comprend les octets d'entête du fichier car celle-ci est dépendante du système d'exploitation de la carte
[18] N représente le nombre de certificat contenus dans l'application « GénériqueCrypto »
[19] N_{Total} représente le nombre total de certificats contenus dans la carte

12 - Annexe D : Règle d'encodage de la longueur d'un objet encapsulé dans un Tag BER-TLV.

Lorsqu'un objet est encapsulé dans un Tag BER-TLV, le champ longueur doit suivre les règles suivantes :

- Si la taille de l'objet est inférieure ou égale à 127 (0x7F), le champ L prend directement la valeur de la taille.
  Exemple : Taille de l'objet sous le tag A5 est 93 (0x5D) : A5 5D < objet>

- Si la taille de l'objet est supérieur ou égale à 128, le champ L est composé de 2 voire 3 octets définis comme suit :
  - L'octet de poids fort est composé de deux digits dont le digit de poids fort prend la valeur 8. Le digit de poids faible fournit le nombre d'octets nécessaires à l'expression de la longueur
  - Le ou les octets suivants expriment la taille de l'objet.

    Exemples :
    Taille de l'objet sous tag A5 est 298 (0x12A) le champ L est alors codé 82 01 2A et l'objet est alors codé : A5 82 01 2A <objet>
    Taille de l'objet sous tag A5 est 128 (0x80) le champ L est codé 81 80 et l'objet est alors codé : A5 81 80 <objet>
    Taille de l'objet sous tag A5 est 178 (0xB2) le champ L est codé 81 B2 et l'objet est alors codé : A5 81 B2 <objet>.