CARTES CPS

Identification version CPS V4

Identification du document	
Référence ANS	ANS_CPSV4_0016_Note_Identification_version_v1_0.docx
Date de création	26/02/2025
Date de dernière mise à jour	
Etat	En cours / A vérifier / A valider / **Validé**
Rédaction (R)	ANS
Version	**V 1.0**
Vérification	
Validation finale (A)	
Classification	**Diffusion restreinte**

Historique du document			
Version	**Date**	**Auteur**	**Commentaires**
V1.0	26/02/2025	ANS/GIE	Création du document

Sommaire

1 Introduction

L'objet de cette note, dédiée à la carte CPS V4, est de décrire comment récupérer la version de la carte CPS V4 qu'on a. Chaque version de carte CPS V4 est associée à un identifiant R4Vx. Cet identifiant indique :

- ✓ La liste des applications présentes ainsi que leur version de logiciel et leur profil de personnalisation
- ✓ La version de plateforme (JCOP)

Pour rappel, la liste des applications est la suivante :

- ✓ Application régalienne (CHIPDOC)
- ✓ Application DESFire
- ✓ Application Emulation CPS2TER
- ✓ Application FIDO

2 Versions de la CPS V4

Ci-dessous, la liste des versions de la CPS V4 :

VERSION	Version TECH	Composant	Profil électrique	Version logicielle
R4V1	0100	Plateforme JCOP		4.5
		Application régalienne CHIPDOC	1.6	4.1.1
		Application Emulation CPS2TER		1.9
		Application DESFire		NP
		Application FIDO		NP
R4V2	0101	Plateforme JCOP		4.5
		Application régalienne CHIPDOC	2.2	4.1.1
		Application Emulation CPS2TER		1.9
		Application DESFire	1.1	EV3c v1.1
		Application FIDO		
R4V3	0102	Plateforme JCOP		4.5
		Application régalienne CHIPDOC	2.3	4.1.1
		Application Emulation CPS2TER		1.9
		Application DESFire	1.1	EV3c v1.1
		Application FIDO		NP

NP : absente et/ou non personnalisée

La colonne Version TECH indique la version de l'identifiant R4Vx, présente dans le fichier TECH décrit en annexe.

3 R4V1 versus R4V2

Différences entre R4V1 et R4V2 :

- Personnalisation du volet DESFire
- Application régalienne CHIPDOC : Modifications liées à la TMAJ et au DESFIRE

4 R4V2 versus R4V3

Différences entre R4V2 et R4V3 :

- Application régalienne CHIPDOC : Identifiants des clés RSA (fichier PKCS#15) identiques à ceux utilisés sur la carte CPS V3 (cela concerne donc les identifiants des clés privées, clés publiques et certificats)
- Application régalienne CHIPDOC : Suppression du fichier PKCS#15 Clé publique ('3F00/0001/7004'), comme sur la V3, ce fichier est personnalisé à 1 octets : '00'
- Application régalienne CHIPDOC : Attribut CKA_UNWRAP des clés privées à FALSE comme sur la V3

5 Identification version carte

L'identification peut se faire :

Au niveau graphique, sur le VERSO de la carte en haut à droite est imprimée la version de la carte :

Au niveau électrique, il faut alors lire le fichier TECH (ID : '3F00/2FFF') de l'application régalienne et récupérer le tag '82' : voir la description de ce fichier en annexe. La lecture de ce fichier peut se faire au travers de la Cryptolib, interface PKCS#11, label object DATA 'TECH'

6 Identification du masque

L'ANS se réserve la possibilité d'avoir des cartes CPS multi sources. L'identification du masque utilisé est réalisée au travers du label du token PKCS#11 (fichier CIAINFO, ID '3F00/0001/5032').

Aujourd'hui, un seul masque existe : NXP P71 / CHIPDOC

Le label du token est : **CPS4v1-xxxxxxxxxx**

Le label est composé du préfixe « CPS4v1- » suivi de l'identifiant logique de la carte contenu dans le fichier EF.ID-CARD, tag '81'

7 Annexes

7.1 Fichier TECH

Le fichier EF TECH est un fichier transparent qui contient des informations sur le profil électrique et graphique de la carte.

Propriété	Valeur
Dénomination fonctionnelle	EF TECH
Identificateur de fichier (chemin complet)	'3F00/**2FFF**'
Type de fichier	EF transparent
Taille du fichier	100
Référence PKCS#11	**TECH**
Attribut de sécurité en contact	Read: ALWAYS Write: NEVER Delete: NEVER

Tag	Length	Description	Value
'F0'	**'4B'**	Tag - Len	
		'**80**0C'	Numéro de support au format 'AAQQQLNNNNNN' où : • AA = millésime (numérique) • QQQ = numéro de jour dans l'année (numérique) • L = identifiant du numéroteur (alphanumérique) • NNNNNN = numéro de séquence dans la journée (numérique)
		'**81**08'	Date d'émission au format ASCII 'AAAAMMJJ'
		'**82**04'	'30313031' : Version du profil au format ASCII (0101)
		'**9F7F**2A'	Valeur du CPLC en fin de perso

Les tags '82' et '81' permettent respectivement d'avoir la version et la date de production de la carte CPS V4.

7.2 Exemple de lecture TECH

Ci-dessous LOG, exemple de lecture du fichier TECH (on passe par l'interface PKCS#11 / Cryptolib) :

```
>>> %Run cpsv4-version.py

Infos slot 0:
=============
 firmwareVersion: 0.00
flags: CKF_TOKEN_PRESENT, CKF_REMOVABLE_DEVICE, CKF_HW_SLOT
hardwareVersion: 0.00
manufacturerID:
slotDescription: OMNIKEY CardMan 5x21 0

Infos token slot 0:
===================
 firmwareVersion: 0.0
flags: CKF_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED
hardwareVersion: 0.0
Label : CPS4v1-3100603747
manufacturerID: ANS
Model : IAS ECC

Get Data Object PKCS#11 (CKA_LABEL = 'TECH'):
=============================================
f04b800c32343135314230303030303033810832303235303231318204303130329f7f2a4790d6004700000000
00409820397921025013124173000041730000000000000000050055042010 74d580000000000000000000000
00000000000000000000000000

Fichier TECH, récupération tags '81' et '82' :
Date    = 20250211
Profile = 0102
[Event-ENDS] No Error.
```