SPECIFICATIONS

Spécifications externes du module PKCS#11

Statut : En cours | *Classification : Public* | *Version : V2.0.1*

AGENCE DU NUMÉRIQUE EN SANTÉ

SOMMAIRE

1 PREAMBULE

1.1. Documents de références

Appellation	Type du document	Nom du document
[R1]	Spécifications	PKCS #11 v2.20: Cryptographic Token Interface Standard
[R2]	Spécifications	ASIP_CPS3_Données-métier_v1.0.2
[R3]	Spécifications	ANS1-001_Profil-Electrique-SSCD-Chipdoc4_v1-3.pdf

1.2. Terminologies et abréviations

Abréviation	Nom du document
CPS	Carte de Professionnel de Santé
GALSS	Gestionnaire d'Accès au Lecteur Santé Social
PSS	Protocole Santé Social
CryptoLib	Ensemble des composants librairie PKCS#11, CSP, CCM, TokenDriver
PC/SC	Personal Computer/Smart Card
CSP	Cryptographic Service Provider
PKCS#11	Standard définissant une interface générique d'accès aux périphériques cryptographiques. (Public Key Cryptographic Standards)
CAPI	Microsoft Cryptography API
CCM	CAPI Certificate Manager
PKCS#15	Cryptographic Token Information Format Standard
IAS ECC	Identification, Authentification, Signature, Carte Européenne du Citoyen
PIN	Personal Identification Number
AMO	Assurance Maladie Obligatoire

2 INTRODUCTION

Le présent document constitue les spécifications externes de la librairie PKCS#11 de la CryptoLib supportant les cartes CPS3 au format IAS ECC ainsi que les cartes CPS4 au format ChipDoc NXP.

2.1. Carte CP3

Une carte CPS3 comporte deux volets possibles pour l'accès aux données et un volet pour les fonctions cryptographiques.
Le volet IAS ECC au format PKCS#15 ainsi que le volet CPS2ter pour les données métiers.

La librairie PKCS#11 assure uniquement le support de la carte CPS3 au travers du volet IAS ECC en utilisant un driver carte IAS.

Afin de se conformer au standard IAS, la CryptoLib doit implémenter les contraintes de ce dernier. Par exemple lors de signature avec hashing, le standard IAS impose que la dernière étape de hashing soit réalisée par la carte à puce.

2.2. Carte CPS4

Une carte CPS4 comporte deux volets possibles pour l'accès aux données et un volet pour les fonctions cryptographiques.

Le volet ChipDoc au format PKCS#15 et volet CPS2ter.

La librairie PKCS#11 assure uniquement le support de la carte CPS4 au travers du volet ChipDoc en utilisant un nouveau driver carte NXP.

La librairie PKCS#11 assure toujours le support de la carte CPS3v3 au travers du volet IAS en utilisant le driver carte CPS3.

La carte CPS4 offre le support de la signature au format RSA-PSS.

L'applet ChipDoc n'offre pas de commande d'apdu Internal Authenticate. Cette commande est remplacée par un déchiffrement RSA de la donnée transmise par l'appelant pour obtenir une signature RSA.

La carte CPS4 offre le support de l'écriture de données sur le fichier CPS_DATA

La carte CPS4 n'offre plus d'interface sans-contact Mifare Classic.

3. TRAITEMENTS SPECIFIQUES DE LA CRYPTOLIB

3.1. Fonctions

3.1.1. Vue d'ensemble

La CryptoLib CPS implémente un sous ensemble des fonctions présentées dans les spécifications PKCS#11 [R1]. De plus certaines fonctions bénéficient d'une implémentation spécifique. La CryptoLib CPS implémente les fonctions du PKCS11 suivant le Tableau 1 et la légende associée **[EX_CPS3_PKCS11_1]**:

Legende	
✓	Implémentation conformément aux spécifications PKCS#11
!	Implémenté de façon spécifique
✗	non implémentée

Categorie	Fonction	Implémentation		Détails
		Carte CPSv3	Carte CPSv4	
Général	C_Initialize	✓	✓	
	C_Finalize	✓	✓	
	C_GetInfo	✓	✓	
	C_GetFunctionList	✓	✓	
Slots & Cartes	C_GetSlotList	✓	✓	
	C_GetSlotInfo	✓	✓	
	C_GetTokenInfo	✓	✓	
	C_WaitForSlotEvent	✓	✓	
	C_GetMechanismList	✓	✓	
	C_GetMechanismInfo	✓	✓	
	C_InitToken	✗	✗	
	C_InitPIN	✓	✓	
	C_SetPIN	✓	✓	
Sessions	C_OpenSession	✓	✓	
	C_CloseSession	✓	✓	
	C_CloseAllSessions	✓	✓	
	C_GetSessionInfo	✓	✓	
	C_GetOperationState	✗	✗	
	C_SetOperationState	✗	✗	
	C_Login	✓	✓	
	C_Logout	✓	✓	
Objets	C_CreateObject	✗	✗	
	C_CopyObject	✗	✗	
	C_DestroyObject	✗	✗	
	C_GetObjectSize	✗	✗	
	C_GetAttributeValue	✓	✓	
	C_SetAttributeValue	!	!	*Ecriture dans le fichier CPS_DATA (CPSv3 et v4)*
	C_FindObjectsInit	✓	✓	
	C_FindObjects	✓	✓	
	C_FindObjectsFinal	✓	✓	
Chiffrement	C_EncryptInit	✓	✓	
	C_Encrypt	✓	✓	
	C_EncryptUpdate	✗	✗	
	C_EncryptFinal	✗	✗	
Déchiffrement	C_DecryptInit	✓	✓	
	C_Decrypt	✓	✓	
	C_DecryptUpdate	✗	✗	
	C_DecryptFinal	✗	✗	
Empreintes	C_DigestInit	✓	✓	
	C_Digest	✓	✓	
	C_DigestUpdate	✓	✓	
	C_DigestKey	✗	✗	
	C_DigestFinal	✓	✓	
Signature	C_SignInit	✓	✓	
	C_Sign	✓	✓	
	C_SignUpdate	✓	✓	
	C_SignFinal	✓	✓	
	C_SignRecoverInit	✗	✗	
	C_SignRecover	✗	✗	
Vérification de signature	C_VerifyInit	✓	✓	
	C_Verify	✓	✓	
	C_VerifyUpdate	✓	✓	
	C_VerifyFinal	✓	✓	
	C_VerifyRecoverInit	✗	✗	
	C_VerifyRecover	✗	✗	
Fonctions dual	C_DigestEncryptUpdate	✗	✗	
	C_DecryptDigestUpdate	✗	✗	
	C_SignEncryptUpdate	✗	✗	
	C_DecryptVerifyUpdate	✗	✗	
Clés	C_GenerateKey	✗	✗	
	C_GenerateKeyPair	✗	✗	
	C_WrapKey	✗	✗	
	C_UnwrapKey	✗	✗	
	C_DeriveKey	✗	✗	
Génération aléatoire	C_SeedRandom	✗	✗	
	C_GenerateRandom	✓	✓	
Fonctions parallèles	C_GetFunctionStatus	✗	✗	
	C_CancelFunction	✗	✗	

Tableau 1

3.1.2. Implémentations spécifiques

3.1.2.1. C_SetAttributeValue

La CryptoLib PKCS#11 permet uniquement la modification de l'attribut CKA_VALUE, et cette dernière n'est réalisable que si le champ CKA_MODIFIABLE de l'objet est positionné à CK_TRUE **[EX_CPS3_PKCS11_9]**.

Remarque : Fonction implémentée uniquement pour pouvoir modifier l'objet « CPS_DATA » qui est le seul objet modifiable sur une carte CPS3 **[EX_CPS3_PKCS11_10]**.

3.1.2.2. C_EncryptInit et C_Encrypt

La CryptoLib CPS implémente uniquement le chiffrement RSA d'un seul bloc par le biais de la clé publique du certificat d'authentification **[EX_CPS3_PKCS11_48]**. Il revient à l'applicatif de conserver les données chiffrées en vue de réaliser plus tard le déchiffrement RSA correspondant.

3.2. Algorithmes

Parmi les algorithmes présentés dans les spécifications PKCS#11 [R1], la CryptoLib CPS supporte uniquement les algorithmes suivants le Tableau 2 **[EX_CPS3_PKCS11_11]** :

Algorithme	Carte CPS3	Carte CPS4
CKM_RSA_PKCS	✓	✓
CKM_SHA1_RSA_PKCS	✓	✓
CKM_SHA256_RSA_PKCS	✓	✓
CKM_RSA_PKCS_PSS	✗	✓
CKM_SHA1_RSA_PKCS_PSS	✗	✓
CKM_SHA256_RSA_PKCS_PSS	✗	✓
CKM_SHA_1	✓	✓
CKM_SHA256	✓	✓

Tableau 2

3.3. Gestion des objets métier CPS

Pour accéder aux objets métier de la carte CPS, l'application doit disposer des labels associés. Ces labels diffèrent en fonction qu'il s'agisse d'une carte CPS3 ou d'une carte CPS4. Ils sont référencés, avec leur dénomination, dans les paragraphes suivants.

3.3.1. Accès

L'accès à certains de ces objets est protégé par code porteur **[EX_CPS3_PKCS11_12]**. Il nécessite donc le login utilisateur. Ces objets sont représentés avec la mention « Accès » à « Protégé » dans le Tableau 3 **[EX_CPS3_PKCS11_13]**. Ils peuvent être « Présent » ou « Absent » selon le type de carte CPS.

3.3.2. Labels des cartes CPS

Label	Dénomination	Accès	CPS3	CPS4
CPS_DATA	Objet de données applicatives	Libre	Présent	Présent
CPS_ID_CARD	Identification carte	Libre	Présent	Présent
CPS_NAME_PS	Caractéristiques porteur	Libre	Présent	Présent

Label	Dénomination	Accès	CPS3	CPS4
CPS_LANG_PS	Codes langues	Libre	Présent	Présent
CPS_INFO_PS	Infos PS2	Libre	Présent	Présent
CPS_ACTIVITY_01_PS	Activité / Situation d'exercice 1	Protégé	Présent	Présent
CPS_ACTIVITY_02_PS	Activité / Situation d'exercice 2	Protégé	Présent	Présent
CPS_ACTIVITY_03_PS	Activité / Situation d'exercice 3	Protégé	Présent	Présent
CPS_ACTIVITY_04_PS	Activité / Situation d'exercice 4	Protégé	Présent	Présent
CPS_ACTIVITY_05_PS	Activité / Situation d'exercice 5	Protégé	Présent	Présent
CPS_ACTIVITY_06_PS	Activité / Situation d'exercice 6	Protégé	Présent	Présent
CPS_ACTIVITY_07_PS	Activité / Situation d'exercice 7	Protégé	Présent	Présent
CPS_ACTIVITY_08_PS	Activité / Situation d'exercice 8	Protégé	Présent	Présent
CPS_ACTIVITY_09_PS	Activité / Situation d'exercice 9	Protégé	Présent	Présent
CPS_ACTIVITY_10_PS	Activité / Situation d'exercice 10	Protégé	Présent	Présent
CPS_ACTIVITY_11_PS	Activité / Situation d'exercice 11	Protégé	Présent	Présent
CPS_ACTIVITY_12_PS	Activité / Situation d'exercice 12	Protégé	Présent	Présent
CPS_ACTIVITY_13_PS	Activité / Situation d'exercice 13	Protégé	Présent	Présent
CPS_ACTIVITY_14_PS	Activité / Situation d'exercice 14	Protégé	Présent	Présent
CPS_ACTIVITY_15_PS	Activité / Situation d'exercice 15	Protégé	Présent	Présent
CPS_ACTIVITY_16_PS	Activité / Situation d'exercice 16	Protégé	Présent	Présent
CPS_SIT_FACT	Situation / Facturation	Protégé	Présent	Présent
CPS_INFO_PS	Caractéristiques professionnelles PS	Libre	Présent	Présent
CPS2TER_ATR	ATR CPS2ter	Libre	Absent	Présent
CPS2TER_ID	Card ID CPS2ter	Libre	Absent	Présent
CPS2TER_ICC	Identification physique CPS2ter	Libre	Absent	Présent
CPS2TER_NAME	Caractéristiques porteur CPS2ter	Libre	Absent	Présent
CPS2TER_LANG	Codes langues CPS2ter	Libre	Absent	Présent
CPS2TER_PSINFO	Infos PS CPS2ter	Libre	Absent	Présent
CPS2TER_DIRAMO	Données AMO	Libre	Absent	Présent
CPS2TER_ACTIVITY_01_PS	Activité / Situation d'exercice 1	Protégé	Présent	Présent
CPS2TER_ACTIVITY_02_PS	Activité / Situation d'exercice 2	Protégé	Présent	Présent
CPS2TER_ACTIVITY_03_PS	Activité / Situation d'exercice 3	Protégé	Présent	Présent
CPS2TER_ACTIVITY_04_PS	Activité / Situation d'exercice 4	Protégé	Présent	Présent
CPS2TER_ACTIVITY_05_PS	Activité / Situation d'exercice 5	Protégé	Présent	Présent
CPS2TER_ACTIVITY_06_PS	Activité / Situation d'exercice 6	Protégé	Présent	Présent
CPS2TER_ACTIVITY_07_PS	Activité / Situation d'exercice 7	Protégé	Présent	Présent
CPS2TER_ACTIVITY_08_PS	Activité / Situation d'exercice 8	Protégé	Présent	Présent
CPS2TER_ACTIVITY_09_PS	Activité / Situation d'exercice 9	Protégé	Présent	Présent
CPS2TER_ACTIVITY_10_PS	Activité / Situation d'exercice 10	Protégé	Présent	Présent
CPS2TER_ACTIVITY_11_PS	Activité / Situation d'exercice 11	Protégé	Présent	Présent
CPS2TER_ACTIVITY_12_PS	Activité / Situation d'exercice 12	Protégé	Présent	Présent
CPS2TER_ACTIVITY_13_PS	Activité / Situation d'exercice 13	Protégé	Présent	Présent
CPS2TER_ACTIVITY_14_PS	Activité / Situation d'exercice 14	Protégé	Présent	Présent
CPS2TER_ACTIVITY_15_PS	Activité / Situation d'exercice 15	Protégé	Présent	Présent
CPS2TER_ACTIVITY_16_PS	Activité / Situation d'exercice 16	Protégé	Présent	Présent

Tableau 3

Les objets de situations d'exercice IAS et CPS2TER peuvent ne pas être contigus dans leur indexation **[EX_CPS3_PKCS11_15B]**.

4. FORMAT

Dans la CryptoLib PKCS#11 de la carte CPS, les objets spécifiques CPS stockés sur la CPS sont remontés tels que lus sur la carte, c'est-à-dire au format ASN.1 **[EX_CPS3_PKCS11_14]**.

Afin d'obtenir un comportement homogène pour les applications, la CryptoLib CPS3 remonte également les objets spécifiques CPS lus sur une carte CPS2Ter dans les objets PKCS#11 CKO_DATA au format ASN.1

[EX_CPS3_PKCS11_15].C'est le rôle de l'application d'adapter le décodage ASN.1 des données métier en fonction du type de carte détectée.

Le format des différents objets de données est décrit dans le document référencé [R2].

5. TRACES

La CryptoLib CPS peut gérer 2 types de traces **[EX_CPS3_PKCS11_16]**:

- Les traces purement PKCS#11.
- Les traces internes à l'implémentation (plus fines).

Remarque : Les données sensibles, telles que le code porteur, ou le code de déblocage, sont masqués **[EX_CPS3_PKCS11_17]**.

5.1. Configuration

La CryptoLib détermine les éléments à tracer en fonction de variables d'environnement présentes dans son contexte d'exécution **[EX_CPS3_PKCS11_18]**.

Il est à la charge de l'utilisateur de la librairie de positionner ces variables.

Pour les traces purement PKCS#11 il faut positionner la variable à « true » **[EX_CPS3_PKCS11_19]**.

Pour les traces internes à l'implémentation, il faut positionner un niveau pouvant aller de 0 à 10 **[EX_CPS3_PKCS11_20]**. Plus ce niveau est élevé, plus les traces sont détaillées **[EX_CPS3_PKCS11_21]**. Il est recommandé d'utiliser le niveau 10 qui trace les données échangées avec la carte.

5.1.1. Windows

Sous Microsoft Windows il faut positionner deux clés de registre en exécutant le fichier « *activation_traces.reg* » situé dans le répertoire d'installation de la CryptoLib, soit :

- `C:\Program Files\santesocial\CPS` pour un installeur CryptoLib 32 bits (resp. 64 bits) sur un OS cible 32 bits (resp. 64 bits)
- `C:\Program Files (x86)\santesocial\CPS` pour un installeur CryptoLib 32 bits sur un OS cible 64 bits.

Le contenu de ce fichier est le suivant **[EX_CPS3_PKCS11_22]**:

```
[HKEY_CURRENT_USER\Software\ASIP Sante\PKCS11]
"Traces"=dword:00000001
"Debug"=dword:0000000a
```

Remarque 1 : Pour désactiver les traces, il faut exécuter le fichier desactivation_traces.reg situé également dans le répertoire d'installation de la CryptoLib. Le contenu de ce fichier est le suivant **[EX_CPS3_PKCS11_23]**:

```
[HKEY_CURRENT_USER\Software\ASIP Sante\PKCS11]
"Traces"=-
"Debug"=-
```

Remarque 2 : Afin d'activer les traces pour tous les utilisateurs, il est nécessaire d'éditer le fichier activation_traces.reg comme suit selon l'architecture de l'installeur CryptoLib utilisé et selon le type d'OS cible **[EX_CPS3_PKCS11_37]**:

- Installeur 32 bits sur un OS 32 bits **[EX_CPS3_PKCS11_38]**:

```
[HKEY_LOCAL_MACHINE\Software\ASIP Sante\PKCS11]
"Traces"=dword:00000001
"Debug"=dword:0000000a
```

- Installeur 32 bits sur un OS 64 bits **[EX_CPS3_PKCS11_39]**:

```
[HKEY_LOCAL_MACHINE\Software\ Wow6432Node\ASIP Sante\PKCS11]
"Traces"=dword:00000001
"Debug"=dword:0000000a
```

- Installeur 64 bits sur un OS 64 bits (embarque les composants Cryptolib 32 bits) **[EX_CPS3_PKCS11_40]**

```
[HKEY_LOCAL_MACHINE\Software\ASIP Sante\PKCS11]
"Traces"=dword:00000001
"Debug"=dword:0000000a

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\ASIP Sante\PKCS11]
"Traces"=dword:00000001
"Debug"=dword:0000000a
```

Remarque 3 : Les paramétrages de traces, s'ils sont configurés pour l'utilisateur courant (HKCU), sont prioritaires sur ceux définis pour tous les utilisateurs (HKLM).

5.1.2. Linux

Sous Linux il existe une manière de positionner les variables nécessaires :

- En positionnant les variables d'environnement comme suit **[EX_CPS3_PKCS11_28]**:
  - export CPS3_PCS11_TRACES=true pour les traces purement PKCS#11.
  - export CPS3_DEBUG=0 à 10 pour les traces internes à l'implémentation.

Remarque : Pour désactiver ces traces, il faut écraser les variables d'environnement comme suit **[EX_CPS3_PKCS11_29]**:

- unset CPS_PKCS11_TRACES
- unset CPS3_DEBUG

5.1.3. macOS

Pour activer les traces sous MAC OS X, il faut éditer le fichier cps3_pkcs11.conf dans le dossier « /Library/Preferences/santesocial/CPS/ » et ajouter les informations suivantes **[EX_CPS3_PKCS11_30]** :

```
traces
{
        active = true;
        debug = 10;
}
```

Remarque : Pour désactiver ces traces, il faut positionner les variables comme suit :

- active = false

- debug = 0

5.2. Emplacement

Les traces sont sauvegardées dans l'emplacement définit par le Tableau 4 **[EX_CPS3_PKCS11_31]**:

Système d'exploitation	Répertoire
Microsoft Windows	%ALLUSERSPROFILE%\santesocial\cps\log
Linux	/var/opt/santesocial/CPS/log/
macOS	~/Library/Logs/santesocial/CPS (~ désigne le répertoire de l'utilisateur)

Tableau 4

6. PARAMETRAGE

6.1. Commande Test Présence Carte

Le paramètre « tpc_polling_time », exprimé en secondes, permet de définir l'intervalle entre deux appels effectifs à la commande lecteur « Test Présence Carte » à travers le Galss pour les lecteurs PSS **[EX_CPS3_PKCS11_32]**.

- Si le paramètre n'est pas défini, sa valeur par défaut est fixée à deux secondes **[EX_CPS3_PKCS11_33]**.
- Si le paramètre est défini, sa valeur sera prise en compte à condition qu'elle soit supérieure à deux secondes **[EX_CPS3_PKCS11_34]**.

6.1.1. Windows

Sous Microsoft Windows, le paramètre doit être positionné en base de registre comme suit pour l'utilisateur courant et quel que soit l'architecture d'OS **[EX_CPS3_PKCS11_35]** :

```
[HKEY_CURRENT_USER\Software\ASIP Sante\PKCS11]
"tpc_polling_time"=dword:00000003
```

Le paramètre « tpc_polling_time » peut être défini comme suit pour 'tous les utilisateurs' selon le type de Cryptolib et l'architecture d'OS **[EX_CPS3_PKCS11_41]**

- CryptoLib 32 bits sur un OS 32 bits **[EX_CPS3_PKCS11_42]** :

```
[HKEY_LOCAL_MACHINE\Software\ASIP Sante\PKCS11]
"tpc_polling_time"=dword:00000003
```

- CryptoLib 32 bits sur un OS 64 bits **[EX_CPS3_PKCS11_43]** :

```
[HKEY_LOCAL_MACHINE\Software\Wow6432Node\ASIP Sante\PKCS11]
"tpc_polling_time"=dword:00000003
```

- CryptoLib 64 bits sur un OS 64 bits (comprend également les composants CryptoLib 32 bits) **[EX_CPS3_PKCS11_44]** :

```
[HKEY_LOCAL_MACHINE\Software\ASIP Sante\PKCS11]
"tpc_polling_time"=dword:00000003

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\ASIP Sante\PKCS11]
"tpc_polling_time"=dword:00000003
```

Remarque 1 : Le paramétrage 'tpc_polling_time', s'il est configuré pour l'utilisateur courant (HKCU), est prioritaire sur celui défini pour tous les utilisateurs (HKLM) **[EX_CPS3_PKCS11_45]**.

6.1.2. Linux et macOS

Sous Linux et MAC OS X, le paramètre doit est positionné dans le fichier cps3_pkcs11.conf comme suit **[EX_CPS3_PKCS11_36]** :

```
Galss
{
        tpc_polling_time = 3;
}
```

6.2. Cache

Les traces sont sauvegardées dans l'emplacement définit par le Tableau 5 **[EX_CPS3_PKCS11_47]**:

Système d'exploitation	Répertoire
Microsoft Windows	%ALLUSERSPROFILE%\santesocial\cps\cache
Linux	/etc/opt/santesocial/CPS/cache/
macOS	/Library/Logs/santesocial/CPS

Tableau 5

6.2.1. macOS

Sous Mac OS X il est possible de modifier l'emplacement du cache en ajoutant un paramètre dans le fichier cps3_pkcs11.conf comme suit **[EX_CPS3_PKCS11_48]**:

```
cache
{
        path = /Chemin/cache;
}
```

7. MATRICE DES EXIGENCES

Exigence	Intitulé	Page
[EX_CPS3_PKCS11_1]	La CryptoLib CPS implémente les fonctions du PKCS11 suivant le Tableau 1 et la légende associée	4
[EX_CPS3_PKCS11_10]	Remarque : Fonction implémentée uniquement pour pouvoir modifier l'objet « CPS_DATA » qui est le seul objet modifiable sur une carte CPS3	6
[EX_CPS3_PKCS11_11]	Parmi les algorithmes présentés dans les spécifications PKCS#11 [R1], la CryptoLib CPS supporte uniquement les algorithmes suivants le Tableau 2	6
[EX_CPS3_PKCS11_12]	L'accès à certains de ces objets est protégé par code porteur	6
[EX_CPS3_PKCS11_13]	Ces objets sont représentés avec la mention « Accès » à « Protégé » dans le Tableau 3	6
[EX_CPS3_PKCS11_14]	Dans la CryptoLib PKCS#11 de la carte CPS, les objets spécifiques CPS stockés sur la CPS sont remontés tels que lus sur la carte, c'est-à-dire au format ASN.1	7
[EX_CPS3_PKCS11_15]	Afin d'obtenir un comportement homogène pour les applications, la CryptoLib CPS3 remonte également les objets spécifiques CPS lus sur une carte CPS2Ter dans les objets PKCS#11 CKO_DATA au format ASN.1	7
[EX_CPS3_PKCS11_15]	La CryptoLib CPS doit être en mesure de lire des situations IAS ou CPS2TER non contiguës dans leur indexation	
[EX_CPS3_PKCS11_16]	La CryptoLib CPS peut gérer 2 types de traces	7
[EX_CPS3_PKCS11_17]	Remarque : Les données sensibles, telles que le code porteur, ou le code de déblocage, sont masqués	7
[EX_CPS3_PKCS11_18]	La CryptoLib détermine les éléments à tracer en fonction de variables d'environnement présentes dans son contexte d'exécution	8
[EX_CPS3_PKCS11_19]	Pour les traces purement PKCS#11 il faut positionner la variable à « true »	8
[EX_CPS3_PKCS11_20]	Pour les traces internes à l'implémentation, il faut positionner un niveau pouvant aller de 0 à 10	8
[EX_CPS3_PKCS11_21]	Plus ce niveau est élevé, plus les traces sont détaillées	8
[EX_CPS3_PKCS11_22]	Le contenu de ce fichier est le suivant	8
[EX_CPS3_PKCS11_23]	Le contenu de ce fichier est le suivant	8
[EX_CPS3_PKCS11_28]	En positionnant les variables d'environnement comme suit	9
[EX_CPS3_PKCS11_29]	Remarque : Pour désactiver ces traces, il faut écraser les variables d'environnement comme suit	9
[EX_CPS3_PKCS11_30]	Pour activer les traces sous MAC OS X, il faut éditer le fichier cps3_pkcs11.conf dans le dossier « /Library/Preferences/santesocial/CPS/ » et ajouter les informations suivantes	9