NOTE DE PUBLICATION

Installation RPM (64b) Cryptolib CPS

Version 5.2.4

Statut : Validé | *Classification : Public* | *Version : V0.1*

AGENCE DU NUMÉRIQUE EN SANTÉ

SOMMAIRE

1 INTRODUCTION

1.1 Objectif du document

L'objectif de ce document est de décrire le périmètre de la dernière version de l'installation RPM pour Linux 64 bits.

1.2 Références

1.2.1 Glossaire

PS	Professionnel de Santé
ES	Etablissement de Santé
CPS	Carte de Professionnel de Santé
RPM	Redhat Package Manager (Package d'installation Linux)
GALSS	Gestionnaire des Accès aux Lecteurs Santé Social

1.2.2 Document de référence

[REF]	Titre	Date
[SPEC]	PSCC_SpecFonct_rpm_cryptolib_190114_v2.1.1	14/01/2019

2 IDENTIFICATION DU PRODUIT

2.1 Propriétés

Propriété	Valeur
Dénomination	CryptolibCPS-5.2.4-1.x86_64.rpm
Version	5.2.4
Type Installeur	RPM
Version installeur (si différente)	-

2.2 Composants

Variable	Valeur
CpsBinDir	/opt/santesocial/CPS/bin/
GalssDir	/usr/local/galss/
CpsLibDir	/opt/santesocial/CPS/lib/
CpsDir	/opt/santesocial/CPS/
CpsConfDir	/etc/opt/santesocial/CPS/
ExtDir	~/.mozilla/firefox/xxx.default/extensions/

Composant	Emplacement	Version	MD5
cpgeslux	*CpsBinDir*	6.08	6490D7D89B311E21C74AB2D210677E3C
libcptablux.so	*GalssDir*	1.08	BC7A4478E75111BB106FE10D8D2A135D
libcps3_pkcs11_lux.so	*CpsLibDir*	3.04	9466DE6B6F5B46023DE536E900EC9B22
DICO-FR.GIP	*CpsConfDir*	2.18	N/A
CPS2ter-2020_Firefox@asipsante.fr	*ExtDir*	6.0.21	N/A
license.txt (LGPL 2.1)	*CpsDir*	2.1	N/A

3 CONFIGURATION REQUISE

3.1 Composants publics

Plateforme	Système d'exploitation		Navigateur	
Linux	RHEL	7	Firefox	128 ESR, 129 à 132
		8	Firefox	128 ESR, 129 à 132
		9	Firefox	128 ESR, 129 à 132

La compatibilité des composants entre eux suit les recommandations définies dans les notes de publications de chacun des composants.

3.2 Autres

Entreprise	Composant	Linux
GIE-SV	GALSS	3.41.00

4 MISES A JOUR DU PRODUIT

4.1 Description

Cette version succède à la version 5.2.3.

4.2 Récapitulatif

E	Evolution	C	Correction

Type	N°	Composant	Descriptif	Depuis
C	1753	Librairie PKC#11 CPS3	Echec d'une signature avec la clé d'authentification avec une CPS4 : Logical channel not supported	5.2.4 07/02/2025
C	1745	Librairie PKC#11 CPS3	Erreur de signature RSA_PKCS avec la clé d'authentification lorsque la longueur demandée est supérieure à 256	
C	1737	Librairie PKC#11 CPS3	Retour de C_GetSlotList KO suite à retrait/insertion d'une CPS	5.2.3 18/11/2024
C	1634	CPS Gestion	Segmentation fault lors de l'utilisation de cpsgeslux	5.2.2 03/09/2024
C	1722	Librairie PKC#11 CPS3	Correction sur la reprise des traitements Cryptolib suite à l'erreur statut carte 69 85 sur la CPS4	5.2.1 21/08/2024
E	1714	Librairie PKC#11 CPS3	Librairie PKCS#11CPS3 compatible CPS3/CPS4	5.2.0 15/07/2024
E	1716	Librairie PKCS#11 CPS3	Implémenter le chiffrement et remonter le flag CKF_ENCRYPT	
E	1712	Librairie PKC#11 CPS3	Exposé des labels PKCS11 pour les données de situation du volet CPS2TER (1 à 16 fichiers)	
E	1638	Extension Firefox	Intégration du XPI CPS 6.0.21	
E	1624	Dictionnaire GIP	Nouveau fichier DICO-FR.GIP v2.18	
C	1605	Librairie PKC#11 CPS3	Carte non détectée suite à une absence de réponse temporaire d'un lecteur PSS	5.1.4 27/09/2019

Type	N°	Composant	Descriptif	Depuis
C	1590	Installeur RPM CPS Gestion	Echec d'installation Cryptolib CPS sur Redhat entreprise linux 8.0	
E	1588	Dictionnaire GIP	Nouveau fichier DICO-FR.GIP v2.15	
C	1574	Librairie PKC#11 CPS3	Retour CKR_TOKEN_NOT_PRESENT au lieu de CKR_GENERAL_ERROR dans certains cas	5.1.2 16/01/2019
E	1572	CPS Gestion	Affichage de la date d'émission pour les CPS3.3	
E	1570	Installeur	Nouveau fichier DICO-FR.GIP v2.13	
E	1389	Installeur RPM	Suppression des composants v4 par l'installeur	
E	1388	Installeur RPM	Les composants v4 ne doivent plus être installés	
E	1542	CPS Gestion	Affichage des situations de facturation	5.0.15 16/04/18
E	1537	Installeur	Evolution d'un suivi des installations déployées (1.29)	
E	1530	Librairie PKC#11 CPS3	Réduction des noms de lecteurs PC/SC par la librairie PKCS11	
C	1528	CPS Gestion	CPS non vue par CPS-Gestion dans un second lecteur PC/SC	
C	1523	CPS Gestion	Correction de l'affichage des CPF dans CPS-Gestion	
C	1520	Installeur	Périphérique de sécurité non installé sous FF58 en Linux 32bits	5.0.14 02/02/18
E	1501	Installeur	Evolution d'un suivi des installations déployées	5.0.13 22/12/17
C	1499	Librairie PKC#11 CPS3	Correction du retour incorrect de C_GetSlotList et C_GestSlotInfo lorsqu'un TLA est débranché	
E	1495	Extension Firefox	Intégration du XPI 6.0.19	

Type	N°	Composant	Descriptif	Depuis
E	1473	Dictionnaire GIP	Nouveau fichier DICO-FR.GIP v2.09	
C	1398	Librairie PKC#11 CPS3 Installeur RPM	Affichage la version d'OpenSC et installation d'une license LGPL 2.1	
C	1466	Librairie PKC#11 CPS3	Compatibilité ascendante du comportement de C_DigestFinal suite à un C_Digest	5.0.12 29/05/17
C	1465	Librairie PKC#11 CPS3	Mise en compatibilité avec OpenSSL Engine pour CKM_RSA_PKCS	
C	1446	CPS Gestion	Les opérations CPS Gestion échouent lorsque la taille des certificats dépasse 2048 octets	5.0.11 15/03/17
E	1444	Extension Firefox	Intégration du dernier XPI 6.0.11	
E	1421	Librairie PKC#11 CPS3	Implémenter la commande PSO Hash Off Card	
E	1408	Dictionnaire GIP	Nouveau fichier DICO-FR.GIP	
C	1133	CPS Gestion CPS2ter	Le nom cpgeslux.old assigné a CPS Gestion CPS2ter est inapprorié	
E	1334	Extension Firefox	Incorporation du XPI Firefox (« Extension CPS » v6.0.9) configuré pour la mise à jour en ligne.	5.0.9 24/12/15
C	1332	Librairie PKC#11 CPS3	Le contexte GALSS n'est pas mis à jour suite au retrait/réinsertion de la carte CPS dans un TLA de version 3.30 ou supérieure.	
C	1175	Librairie PKC#11 CPS3	Impossible d'identifier une carte CPS3 bloquée lorsque le nombre de maximum de déblocage a été atteint.	
C	1226	Librairie PKC#11 CPS3	Lecture superflue des données de l'objet CPS_DATA lors d'un appel C_GetAttributeValue() pour demander uniquement la taille des données	

Type	N°	Composant	Descriptif	Depuis
E	1200	Dictionnaire GIP	Nouvelle version du fichier DICO : 2.06	
E	1232	Librairie PKC#11 CPS3 Librairie PKC#11 CPS2ter Librairie CPS Librairie PKCS#11 Full PC/SC CPS2ter	Adaptation au nouveau comportement de Openssl 1.0.1k	5.0.7 09/04/2015
C	1172	Installeur RPM	La désinstallation ne supprime pas les fichiers contenus dans le répertoire des logs	5.0.6 31/07/14
C	1171	Installeur RPM	Installation RPM v5 sur RPM Full PC/SC	
C	1170	Installeur RPM	Installation v5 sur ancienne version	
C	1160	Installeur RPM	Problème de positionnement de droits sur les fichiers de configuration	
E	1155	Librairie PKCS#11 CPS3	Amélioration du paramétrage de la Cryptolib CPS v5	
C	1144	Librairie PKCS#11 CPS3	Ouverture de sessions GALSS sans les refermer	
C	1141	CPS Gestion	Blocage de CPS-Gestion sur la fonction C_GenerateRandom() avec la carte MAXIMA	
C	1128	CPS Gestion	CPS Gestion ne vérifie pas que le PIN saisi est numérique.	
C	1089	Librairie PKCS#11 CPS3	Mauvais retour de C_GetSlotInfo pour une carte à l'envers dans un lecteur PSS	
C	1071	Librairie PKCS#11 CPS3	Transactions PC/SC ouvertes à vide lorsque le cache est utilisé	

Type	N°	Composant	Descriptif	Depuis
C	1102	Librairie PKCS#11 CPS3	Si un fichier de cache généré par la Cryptolib CPS3 était altéré, la carte CPS3 était alors inexploitable	5.0.4 31/10/13
C	1088 & 1090	Librairie PKCS#11 CPS3	En contexte sans contact, l'accès à la clé privée du certificat technique nécessitait la présentation du code porteur. Or dans la partie sans contact, il n'existe pas de code porteur Il en découlait que : • Il n'était plus possible de signer avec la clé privée associée au certificat technique Il n'était pas possible d'initier une connexion SSL car un code porteur était demandé, alors qu'il n'en existait pas.	
E	1079	Installeur RPM	Cette évolution consiste à intégrer les nouveaux certificats de l'IGC SANTE dans les installeurs de la Cryptolib CPS	
E	1076	Extension Firefox	Cette évolution consiste à positionner un libellé générique associé à la CryptoLib dans la liste des modules de sécurité dans Firefox. Le nouveau libellé est : « *Module de sécurité CPS* » • Les nouveaux certificats de l'IGC SANTE sont également ajoutés dans la base de certificat de Firefox	
C	1068	Librairie PKCS#11 CPS3	Lorsque les traces de la CryptoLib CPS3 étaient activées, certaines traces non conformes à la nomenclature étaient injectées	
E	1056	Extension Firefox	Extension CPS non reconnue à partir de la version 21 de Firefox.	5.0.3 23/04/13
E	1040	Installeur	Supprimer la dépendance au RPM Galss	5.0.2 15/03/13
E		Librairie PKCS#11 CPS3	Adaptations de fonctionnement pour être davantage conforme à la spécification PKCS#11 v2.20	5.0.1 30/10/12

Type	N°	Composant	Descriptif	Depuis
E	974	Extension Firefox	Le XPI n'installe plus le certificat d'inscription dans la base de certificats Firefox. Si ce certificat est déjà présent dans la base, le XPI 6.0.1 le supprime au 1er lancement de Firefox.	
E	945	Installeur	Suppression du certificat d'inscription en tant que composant dans les installeurs Cryptolib CPS	
C	8401 814	API CPS	Re-sélectionner l'application CPS IAS en cas d'erreur 6E00	

5 PROBLEMES IDENTIFIES, CONSEILS ET PALLIATIFS