



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NOTE DE PUBLICATION | | | | |
| Installation PKG Cryptolib CPS | | | | |
| Version 5.2.0 | | | | |
| Statut : Validé | | | Classification : Public | | | Version : V0.1 |

Historique du document

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Rédigé par | | Vérifié par | | Validé par | |
| 0.1 | ASIP | Le 18/04/2019 | ASIP | Le 18/04/2019 | ASIP | Le 18/04/2019 |
| Motif et nature de la modification : Création du document | | | | | |
| Motif et nature de la modification : | | | | | |

**SOMMAIRE**

[1 Introduction 2](#_Toc171002384)

[1.1 Objectif du document 2](#_Toc171002385)

[1.2 Références 2](#_Toc171002386)

[1.2.1 Glossaire 2](#_Toc171002387)

[1.2.2 Document de référence 2](#_Toc171002388)

[2 Identification du produit 3](#_Toc171002389)

[2.1 Propriétés 3](#_Toc171002390)

[2.2 Composants 3](#_Toc171002391)

[3 Configuration requise 4](#_Toc171002392)

[3.1 Composants publics 4](#_Toc171002393)

[3.2 Autres 4](#_Toc171002394)

[4 Mises à jour du produit 5](#_Toc171002395)

[4.1 Description 5](#_Toc171002396)

[4.2 Récapitulatif 5](#_Toc171002397)

[5 Problèmes identifiés, conseils et palliatifs 16](#_Toc171002398)

[1.1. CPS Gestion n’affiche pas les informations de la carte CPS 16](#_Toc171002399)

# Introduction

## Objectif du document

L’objectif de ce document est de décrire le périmètre de la dernière version de l’installation PKG pour macOS.

## Références

### Glossaire

|  |  |
| --- | --- |
| **PS** | Professionnel de Santé |
| **ES** | Etablissement de Santé |
| **CPS** | Carte de Professionnel de Santé |
| **PKG** | macOS Installer (Package d’installation macOS) |
| **Framework** | Bibliothèque macOS |
| **GALSS** | Gestionnaire des Accès aux Lecteurs Santé Social |

### Document de référence

|  |  |  |
| --- | --- | --- |
| **[REF]** | Titre | Date |
| **[SPEC]** | PSCC\_SpecFonct\_pkg\_cryptolib\_230106\_v2.1.6 | 06/01/2023 |
|  |  |  |

# Identification du produit

## Propriétés

|  |  |
| --- | --- |
| **Propriété** | **Valeur** |
| Dénomination | CryptolibCPS-5.2.0.dmg |
| Version | 5.2.0 |
| Type Installeur | PKG |
| Version installeur  (si différente) | - |

## Composants

|  |  |
| --- | --- |
| **Variable** | **Valeur** |
| AppDir | /Applications/ |
| PrefsDir | /Library/Preferences |
| PrefPanes | /Library/PreferencePanes |
| MozExtDir | ~/Library/Application Support/Firefox/Profiles/\*.default/extensions |
| LibDir | /usr/local/lib |
| Frameworks | /Library/Frameworks |
| SupportDir | /Library/Application Support/santesocial/CPS |

| **Composant** | **Emplacement** | **Version** | **MD5** |
| --- | --- | --- | --- |
| cpgesosx.app | *AppDir* | 6.09 | 8AF951D5EC9751BB15B5B66C32A6DD76 |
| cptabosx.framework | *Frameworks* | 5.13 | 2A3B0265110B0BD81C871E3BFBFCDEDD |
| DICO-FR.GIP | *PrefsDir* | 2.18 | - |
| libcps3\_pkcs11\_osx.dylib | *LibDir* | 3.0 | 7038E104C305F0B5C2F4DDA9568A4C4D |
| CPS2ter-2020\_Firefox@asipsante.fr | *MozExtDir* | 6.0.21 | - |
| uninstall.sh | *SupportDir* | 14/05/18 | - |
| PrefsCPS.prefpane | *PrefPanes* | 2.0 | A8420E95F2693A9ADE6C50C0C8AA0A9C |

# Configuration requise

## Composants publics

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Plateforme** | **Système d‘exploitation** | | | **Navigateur** | | |
| **Mac** | macOS | 12 |  | Safari | 16 et 17 |  |
|  |  |  |  | Firefox | 115 ESR, 124 à 127 |  |
|  |  |  |  | Chrome | 123 à 126 |  |
|  |  | 13 |  | Safari | 16 et 17 |  |
|  |  |  |  | Firefox | 115 ESR, 124 à 127 |  |
|  |  |  |  | Chrome | 123 à 126 |  |
|  |  | 14 |  | Safari | 16 et 17 |  |
|  |  |  |  | Firefox | 115 ESR, 124 à 127 |  |
|  |  |  |  | Chrome | 123 à 126 |  |

|  |  |
| --- | --- |
| C:\Users\jmetzger\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\VZX3QJXN\MC900293188[1].wmf | La compatibilité des composants entre eux suit les recommandations définies dans les notes de publications de chacun des composants. |

## Autres

|  |  |  |
| --- | --- | --- |
| **Entreprise** | **Composant** | **Mac** |
| GIE-SV | GALSS | 3.42.03 |

# Mises à jour du produit

## Description

Cette version succède à la version 5.1.20.

## Récapitulatif

*Les lignes en texte « masqué » sont non publiques.*

|  |  |  |  |
| --- | --- | --- | --- |
| **E** | **Evolution** | **C** | **Correction** |

| **Type** | **N°** | **Composant** | **Descriptif** | **Depuis** |
| --- | --- | --- | --- | --- |
| **E** | **1720** | **Librairie PKCS#11 CPS3** | Librairie PKCS#11 CPS3 compatible CPS3/CPS4 | 5.2.0  01/07/2024 |
| **E** | **1716** | **Librairie PKCS#11 CPS3** | Implémenter le chiffrement et remonter le flag CKF\_ENCRYPT |  |
| **E** | **1711** | **Librairie PKCS#11 CPS3** | Exposé des labels PKCS11 pour les données de situation du volet CPS2TER (1 à 16 fichiers) |  |
| **E** | **1678** | **Préférences CPS** | Demande d'évolution pour le stockage et la récupération des Logs sous macOS 12.4 | 5.1.20  06/03/2023 |
| **E** | **1667** | **Installeur** | Diminuer le nombre de saisies du mot de passe admin à l'installation | 5.1.19  02/17/2021 |
| **C** | **1666** | **Installeur** | Comportement de la WebExtension de désactivation sous macOS BigSur Intel |  |
| **E** | **1663** | **Installeur** | Composants « Full Universal binary » | 5.1.16  03/12/2021 |
| **E** | **1658** | **CPS Gestion** | Compatibilité Apple Silicon & 64 bits | 5.1.13  12/10/2021 |
| **E** | **1639** | **Extension Firefox** | Activation/désactivation du module de sécurité depuis le menu de la WebExtension CPS |  |
| **E** | **1637** | **Librairie PKC#11 CPS3** | Compatibilité Apple Silicon & 64 bits | 5.1.11  15/03/2021 |
| **E** | **1625** | **DICO-FR.GIP** | Nouveau fichier DICO-FR.GIP v2.18 |  |
| **E** | **1603** | **Tous** | Support de la notarisation pour macOS Catalina (10.15) | 5.1.8  10/09/2019 |
| **C** | **1598** | **Librairie PKC#11 CPS3** | Carte non détectée suite à une absence de réponse temporaire d'un lecteur PSS | 5.1.6  18/07/2019 |
| **E** | **1597** | **TokenD** | Compatibilité TokenD et token Driver |  |
| **E** | **1596** | **Tous** | Passage des composants en Full 64b |  |
| **C** | **1583** | **Installeur** | Adaptation de l'installation de l'extension CPS à Firefox 67 Beta sous Mac | 5.1.5  11/04/2019 |
| **C** | **1573** | **Librairie PKC#11 CPS3** | Retour CKR\_TOKEN\_NOT\_PRESENT au lieu de CKR\_GENERAL\_ERROR dans certains cas | 5.1.4  14/01/2019 |
| **E** | **1572** | **CPS Gestion** | Affichage de la date d'émission pour les CPS3.3 |  |
| **E** | **1569** | **DICO-FR.GIP** | Nouveau fichier DICO-FR.GIP v2.13 |  |
| **E** | **1384** | **Installeur** | Les composants v4 ne doivent plus être installés |  |
| **E** | **1383** | **Installeur** | Suppression des composants v4 par l'installeur |  |
| **E** | **1304** | **TokenD** | Mise en conformité "Apple" de l'intégrité du TokenD |  |
| **C** | **1549** | **TokenD** | Support du SHA512 via les CPS 3.3 | 5.0.41  05/06/2018 |
| **E** | **1541** | **CPS Gestion** | Affichage des situations de facturation | 5.0.40  15/05/2018 |
| **E** | **1536** | **Installeur** | Evolution d'un suivi des installations déployées (1.29) |  |
| **E** | **1532** | **Librairie**  **PKC#11 CPS3** | Réduction des noms de lecteurs PC/SC par la librairie PKCS11 |  |
| **C** | **1527** | **Driver Galss** | Avec 2 lecteurs PSS, 1 seul est remonté par le Tokend |  |
| **C** | **1525** | **Installeur** | L'extension CPS 6.0.19 n'est pas reconnue par Firefox 59b si elle est déployée par l'installeur PKG | 5.0.39  13/02/2018 |
| **C** | **1522** | **CPS Gestion** | Correction de l'affichage des CPF dans CPS-Gestion |  |
| **E** | **1518** | **Driver Galss** | Optimisation de la configuration par défaut du délai de démarrage |  |
| **E** | **1500** | **Installeur** | Evolution d'un suivi des installations déployées (1.27) | 5.0.38  19/12/2017 |
| **C** | **1498** | **Librairie**  **PKC#11 CPS3** | Correction du retour de C\_GetSlotList et de C\_GestSlotInfo lorsqu’un TLA est débranché |  |
| **E** | **1493** | **Installeur** | Intégration du XPI 6.0.19 |  |
| **C** | **1488** | **Librairie**  **PKC#11 CPS3** | Compatibilité ATSAM v4 | 5.0.36  21/11/2017 |
| **E** | **1472** | **DICO-FR.GIP** | Nouveau fichier DICO-FR.GIP v2.09 | 5.0.35  01/08/2017 |
| **C** | **1468** | **Extension Firefox** | Intégration du dernier XPI 6.0.15 compatible avec Firefox 55 |  |
| **C** | **1397** | **Librairie**  **PKC#11 CPS3** | Affichage la version d’OpenSC et license LGPL 2.1 |  |
| **E** | **1385** | **Installeur** | Intégration d’un suivi des installations |  |
| **C** | **1365** | **Tous** | Supprimer les références à Xcode dans les info.plist |  |
| **C** | **1342** | **Installeur** | Les répertoires /Library/Caches/santesocial/CPS/ et /Library/Logs/santesocial/CPS/ ne sont pas backupés |  |
| **C** | **1326** | **Cptab** | Problèmes avec les bundles Frameworks |  |
| **C** | **1321** | **Tous** | L'utilisation des fichiers PkgInfo n'est pas cohérente |  |
| **C** | **1320** | **Tous** | CFBundleIdentifier n'est pas systématiquement utilisé |  |
| **C** | **1319** | **Tous** | Le champ CFBundleSignature n'est pas systématiquement positionné |  |
| **C** | **1301** | **Librairie PKC#11 CPS3,**  **TokenD,**  **Driver Galss** | Les logs ne sont pas créés sous El Capitan final |  |
| **C** | **1464** | **Librairie PKC#11 CPS3** | Compatibilité ascendante du comportement de C\_DigestFinal suite à un C\_Digest | 5.0.34  22/05/2017 |
| **C** | **1463** | **Librairie PKC#11 CPS3** | Mise en compatibilité avec OpenSSL Engine pour CKM\_RSA\_PKCS |  |
| **C** | **1445** | **CPS Gestion** | Les opérations CPS Gestion échouent lorsque la taille des certificats dépasse 2048bytes | 5.0.33  14/03/2017 |
| **E** | **1442** | **Extension Firefox** | Intégration du dernier XPI 6.0.11 |  |
| **E** | **1420** | **Librairie PKC#11 CPS3** | Implémenter la commande PSO Hash Off Card |  |
| **E** | **1417** | **Librairie PKC#11 CPS3** | Accès au DAM |  |
| **C** | **1411** | **Scripts** | Le script postinstall.command est corrompu |  |
| **C** | **1372** | **TokenD** | Problème d’authentification lors de la connexion SSL avec Chrome sous macOS Sierra |  |
| **C** | **1346** | **Extension Firefox** | Problème d'installation du XPI 6.0.9 sous Mac OS X |  |
| **C** | **1330** | **Installeur PKG** | L'intégration de modutil dans l'installeur est à revoir |  |
| **C** | **1328** | **Scripts** | Fautes de français dans le script common.sh + postX.sh |  |
| **C** | **1327** | **Installeur PKG** | L'installeur Cryptolib CPS pour Mac OS X est trop volumineux |  |
| **C** | **1323** | **Composants**  **CPS2ter** | cptabosx et sscasosx embarquent toujours un binaire PPC |  |
| **C** | **1316** | **Composants**  **CPS2ter** | Le framework CPTABOSX pour Mac OS X contient 3 versions différentes de la librairie cptabosx |  |
| **C** | **1313** | **Installeur PKG** | Duplication de ressources dans l'installeur PKG Mac OS X |  |
| **C** | **1284** | **CPS Gestion** | Mauvais nom de bundle du CPS Gestion v5 |  |
| **E** | **1407** | **DICO-FR.GIP** | Nouveau fichier DICO-FR.GIP | 5.0.30  04/08/2016 |
| **E** | **1400** | **Driver Galss** | Augmentation du StartUpDelay |  |
| **E** | **1395** | **Installeur PKG** | Mettre à jour le script uninstall.sh |  |
| **C** | **1371** | **TokenD** | Problème d’authentification lors de la connexion SSL avec Safari 10 |  |
| **C** | **1367** | **TokenD** | Les valeurs de CFBundleShortVersionString et CFBundleVersion sont différentes dans le tokend |  |
| **C** | **1366** | **Driver Galss** | Les valeurs de CFBundleShortVersionString et CFBundleVersion sont différentes dans le GALSSDriver |  |
| **C** | **1322** | **Driver Galss** | Le GALSS Driver embarque toujours un binaire PPC |  |
| **C** | **1312** | **TokenD** | Les champs CFBundlePackageType des Info.plist du TokenD CPS3 sont incorrects |  |
| **C** | **1302** | **TokenD** | Les PID et TID des fichiers CPS3Tokend\_[PID]\_[TID].log sont en décimal au lieu d'être en hexadecimal |  |
| **C** | **1295** | **Driver Galss** | Le fichier GALSS Driver Info.plist embarqué n'est pas celui fourni par le GIE-SV |  |
| **C** | **1289** | **TokenD** | Le code PIN sort en clair dans les traces TokenD |  |
| **C** | **1286** | **TokenD** | Le TokenD utilise CKA\_LABEL plutôt que les usages puis CKA\_ID pour chercher les certificats dans le PKCS11 |  |
| **C** | **1283** | **TokenD** | Mauvais nom de bundle du TokenD |  |
| **C** | **1282** | **Driver Galss** | Mauvais nom de bundle du GALSS Driver |  |
| **E** | **1281** | **TokenD** | Les sources du TokenD ne sont pas organisées correctement |  |
| **C** | **1349** | **Librairie PKC#11 CPS3** | Les composants 32b ne sont pas installés par la version 5.0.21 | 5.0.24  12/02/2016 |
| **C** | **1345** | **Librairie PKC#11 CPS3** | Changement de version du compilateur Mac OS X | 5.0.21  22/12/2015 |
| **E** | **1334** | **Extension Firefox** | Incorporation du XPI Firefox (« Extension CPS »  v6.0.9) configuré pour la mise à jour en ligne. |  |
| **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** | **1263** | **Extension Firefox** | Incorporation du XPI Firefox (« Extension CPS » v6.0.8 déclarant le « Module de sécurité CPS » et installant les certificats des IGC de Santé CPS2Bis, CPS2Ter et PFCNG) signé par la Mozilla conformément aux nouvelles mesures de sécurité introduites par Firefox 41. | 5.0.19  10/09/15 |
| **C** | **1262** | **Installeur PKG** | Impossible d'ajouter les certificats root et AC de l'ASIP dans les Keychains du système. |  |
| **C** | **1261** | **Librairie PKC#11 CPS3** | Les certificats CPS sont remontés dans le trousseau uniquement si CPS Gestion ou Firefox est ouvert. |  |
| **E** | **1255** | **Galss Driver** | Incorporation du fichier info.plist fourni par le GIE-SV pour ses lecteurs PSS. |  |
| **C** | **1245** | **Installeur PKG** | L’installation des composants CryptolibCPS échoue sur OS X 10.11 Developer Preview. |  |
| **C** | **1244** | **TokenD** | Support des lecteurs PSS à travers une interface PC/SC. |  |
| **C** | **1226** | **Librairie PKC#11 CPS3** | Correction dans la lecture des données de l'objet CPS\_DATA lors d'un appel C\_GetAttributeValue() avec pointeur NULL. |  |
| **C** | **1206** | **Extension Firefox** | Extension CPS 6.0.2 non reconnue par Firefox 34 en version Beta sous Mac. |  |
| **E** | **1204** | **Installeur PKG** | Supprimer le lancement automatique au démarrage du Resource Manager PC/SC. |  |
| **E** | **1201** | **Librairie PKC#11 CPS3** | Modifier l'emplacement du dossier cache. |  |
| **E** | **1200** | **Fichier DICO** | Déploiement d’un nouveau fichier DICO. |  |
| **C** | **1199** | **Librairie PKC#11 CPS3** | La carte dans le lecteur n'est pas vue si la librairie PKCS#11 CPS3 n'a pas accès au dossier cache. |  |
| **C** | **1192** | **Librairie PKC#11 CPS4** | Le changement de carte dans CPS Gestion ne fonctionne pas. |  |
| **C** | **1187** | **TokenD** | Les certificats de la carte CPS3 ne sont pas ajoutés dans le trousseau de clés. |  |
| **C** | **1175** | **Librairie PKC#11 CPS3** | Correction dans le mécanisme de détection de carte CPS3 bloquée lorsque le nombre de maximum de déblocage a été atteint. |  |
| **E** | **1232** | **Librairie PKCS#11 CPS3**  **Librairie PKCS#11 CPS2ter Galss**  **Librairie API CPS** | Adaptation au nouveau comportement de OpenSSL 1.0.1k | 5.0.15  02/04/15 |
| **E** | **1178** | **Installeur PKG** | Intégration d'un script de désinstallation MacOS | 5.0.12  30/07/14 |
| **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** | **1117** | **Installeur PKG** | Supprimer l'adhérence au Galss lors de l’installation de la Cryptolib CPS3 |  |
| **C** | **1116** | **TokenD** | L'utilisation de la clé de signature en sans contact sous Safari nécessite la saisie d'un code porteur. |  |
| **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 |  |
| **C** |  |  | La version affichée sur l’installeur n’est pas à jour |  |
| **C** |  |  | Les composants binaires v4 ne sont pas corrects |  |
| **C** | **1102** | **Librairie PKCS#11 CPS3** | Si un fichier de cache généré par la Cryptolib CPS3 était altéré, la carte CPS3 était alors inexploitable | 5.0.7  26/11/13 |
| **E** | **1104** | **Librairie PKCS#11 CPS3** | Cette évolution permet de supporter la signature d'un condensat avec une carte CPS3 |  |
| **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 PKG** | 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 était non reconnue à partir de la version 21 de Firefox. | 5.0.4  06/05/13 |
| **C** | **962 (945)** | **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. | 5.0.3  30/10/2012 |
| **C** | **8401 814** | **API CPS** | Re-sélectionner l'application CPS IAS en cas d'erreur 6E00 |  |
| **C** |  | **Extension Firefox** | Le nom affiché de l’extension IGC 2020 dans Firefox est « Extension CPS » |  |
| **E** |  | **Module PKCS#11 CPS 3** | Adaptations de fonctionnement pour être d’avantage conforme à la spécification PKCS#11 v2.20 |  |
| **C** | **958** | **Installeur PKG** | L'installeur PKG 5.0.3 n'installe plus le certificat d'inscription dans le répertoire Coffre. |  |
| **E** |  | **Installeur PKG** | Installation des certificats racines et intermédiaires de l’IGC CPS2ter2020 | 5.0.2  11/05/2012 |
| **E** |  | **Extension Firefox** | Une nouvelle extension « Composants Cryptographiques CPS v6.0 » est installée. Elle déploie les certificats racines et intermédiaires de l’IGC CPS2ter2020 dans Mozilla Firefox. |  |
| **E** |  | **Cryptolib** | Mise à jour du fichier DICO-FR.GIP (v2.02). |  |

# Problèmes identifiés, conseils et palliatifs

## CPS Gestion n’affiche pas les informations de la carte CPS

Si le mode d’apparence « Sombre » est activé sous macOS, les informations de la carte affichées par CPS Gestion sont invisibles. Basculer en mode d’apparence « Clair » pour rendre les informations visibles.

Le paramétrage du mode d’apparence est accessible dans la section « Général » des « Préférences Système ».