# NOTE DE PUBLICATION

## Installation Cryptolib CPS

Version 5.2.7 32 bits et 64bits

*Statut : Validé* | *Classification : Public* | *Version : V0.3*

AGENCE DU NUMÉRIQUE EN SANTÉ

# SOMMAIRE

1 Introduction ..... 2
1.1 Objectif du document ..... 2
1.2 Références ..... 2
*1.2.1 Glossaire ..... 2*
*1.2.2 Document de référence ..... 2*
2 Identification du produit ..... 3
2.1 Propriétés ..... 3
2.2 Composants ..... 3
3 Configuration requise ..... 5
3.1 Composants publics ..... 5
3.2 Autres ..... 5
4 Mises à jour du produit ..... 6
4.1 Description ..... 6
4.2 Récapitulatif ..... 6
5 Problèmes identifiés, conseils et palliatifs ..... 8
5.1 Note concernant les patchs FIDO2 ..... 8
*5.1.1 Cas d'usage et mode d'activation ..... 8*
*5.1.2 Patch P1 ..... 9*
*5.1.3 Patch P2 ..... 9*
*5.1.4 Patch P3 ..... 9*
*5.1.5 Patch P4 ..... 9*



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

# 1 INTRODUCTION

## 1.1 Objectif du document

L'objectif de ce document est de décrire le périmètre des dernières versions 32 et 64 bits de l'installation de la Cryptolib CPS sous Windows.

## 1.2 Références

### 1.2.1 Glossaire

| | |
|---|---|
| **PS** | Professionnel de Santé |
| **ES** | Etablissement de Santé |
| **CPS** | Carte de Professionnel de Santé |
| **MSI** | Microsoft Windows Installer (Package d'installation Microsoft) |
| **DLL** | Dynamic Link Library (bibliothèque à liens dynamiques) |
| **GALSS** | Gestionnaire des Accès aux Lecteurs Santé Social |
| **UAC** | User Account Control |
| **EPM** | Enhanced Protected Mode |
| **CSP** | Cryptographic Service Provider |

### 1.2.2 Document de référence

| [REF] | Titre | Date |
|---|---|---|
| **[SPEC]** | *PSCC_SpecFonct_exe_cryptolib_170123_v1.0.0* | 23/01/2017 |
| **[SPEC]** | *PSCC_SpecFonct_msi_cryptolib_240625_v3.3.4.doc* | 25/06/2024 |
| **[CREQ]** | | |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

# 2 IDENTIFICATION DU PRODUIT

## 2.1 Propriétés

| Propriété | Valeur |
|---|---|
| Dénomination | CryptolibCPS-5.2.7.exe (installeur 32 et 64 bits) |
| Version | 5.2.7 |
| Type Installeur | Setup EXE |
| Version installeur (si différente) | |

## 2.2 Composants

| Variable | Valeur |
|---|---|
| %InstallDir% | C:\Program Files\santesocial\CPS |
| %InstallDir_64% | |
| %InstallDir_32% | C:\Program Files (x86)\santesocial\CPS |
| %SysDir% | C:\Windows\system32 |
| %SysDir_64% | |
| %SysDir_32% | C:\Windows\SysWOW64 |
| %ProfilesDir% | %APPDATA%\Mozilla\Firefox\Profiles |
| %ExtDir% | %ProfilesDir%\<dossier du profil>\extensions |
| %WinDir% | C:\Windows |
| %SanteSocial% | XP et 2003 TSE / Citrix :<br>%ALLUSERSPROFILE%\Application Data\santesocial\<br>Vista / W7 / Serveur 2008 :<br>%ALLUSERSPROFILE%\santesocial\ |
| %Coffre% | %SanteSocial%\cps\coffre |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

| Composant | Emplacement | Version | MD5 |
|---|---|---|---|
| **Sur une plateforme 32 bits** | | | |
| CCM.exe | *%InstallDir%* | 3.14.0 | 9B02CBDDDFFDCB1ED7C21CE5FE742E1C |
| cpgesw32.exe | *%InstallDir%* | 6.9.0 | 62D797599B4F78619E4BF50428036CF2 |
| cps3_csp_w32.dll | *%SysDir%* | 3.9.0 | 73511C96E3E1ADF99DBB4F7425F0ED6C |
| cps3_pkcs11_w32.dll | *%SysDir%* | 3.8.0 | 082B956A3F4C3576D48A2ECC7A38EC24 |
| cptabw32.dll | *%WinDir%* | 5.6.0 | 3B2F41D8374D0D25399124227EB71F78 |
| CPS2ter-2020_Firefox@asipsante.fr | *%ExtDir%* | 6.0.21 | - |
| activation_traces.reg | *%InstallDir%* | - | - |
| desactivation_traces.reg | *%InstallDir%* | - | - |
| DICO-FR.GIP | *%WinDir%*<br>*%Coffre%* | 2.18 | - |
| **Sur une plateforme 64 bits** | | | |
| CCM.exe | *%InstallDir_64%* | 3.14.0 | 1F3D1633503FC0940F161E466C9C9AAA |
| cpgesw32.exe | *%InstallDir_32%* | 6.9.0 | 62D797599B4F78619E4BF50428036CF2 |
| cpgesw64.exe | *%InstallDir_64%* | 6.9.0 | 752D68EAF1970FDB4BB8B0B41E3BA28D |
| cps3_csp_w32.dll | *%SysDir_32%* | 3.9.0 | 73511C96E3E1ADF99DBB4F7425F0ED6C |
| cps3_csp_w64.dll | *%SysDir_64%* | 3.9.0 | B3A51530D75EF91964329BDFEBE707DC |
| cps3_pkcs11_w32.dll | *%SysDir_32%* | 3.8.0 | 082B956A3F4C3576D48A2ECC7A38EC24 |
| cps3_pkcs11_w64.dll | *%SysDir_64%* | 3.8.0 | 08E196560155324B4C6AA1D7A295288D |
| cptabw32.dll | *%WinDir%* | 5.6.0 | 3B2F41D8374D0D25399124227EB71F78 |
| cptabw64.dll | *%WinDir%* | 5.6.0 | 777EA2662389BF2F33384EB80283A03E |
| CPS2ter-2020_Firefox@asipsante.fr | *%ExtDir%* | 6.0.21 | - |
| activation_traces.reg | *%InstallDir_64%* | - | - |
| desactivation_traces.reg | *%InstallDir_64%* | - | - |
| DICO-FR.GIP | *%WinDir%*<br>*%Coffre%* | 2.18 | - |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

# 3 CONFIGURATION REQUISE

## 3.1 Composants publics

| Plateforme | Système d'exploitation | | | Navigateur | | |
|---|---|---|---|---|---|---|
| Windows | 10 | | | Edge Chromium | 146 à 150 | |
| | | | | Firefox | 140 ESR, 149 à 153 | |
| | | | | Chrome | 146 à 153 | |
| | 11 | | | Edge Chromium | 146 à 150 | |
| | | | | Firefox | 140 ESR, 149 à 153 | |
| | | | | Chrome | 146 à 153 | |
| | Server 2016 TSE / CITRIX 1808 | | | Edge Chromium | 146 à 150 | |
| | | | | Firefox | 140 ESR, 149 à 153 | |
| | | | | Chrome | 146 à 153 | |
| | Server 2019 TSE / CITRIX 1906 | | | Edge Chromium | 146 à 150 | |
| | | | | Firefox | 140 ESR, 149 à 153 | |
| | | | | Chrome | 146 à 153 | |
| | Server 2022 TSE / CITRIX 1906 | | | Edge Chromium | 146 à 150 | |
| | | | | Firefox | 140 ESR, 149 à 153 | |
| | | | | Chrome | 146 à 153 | |

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

## 3.2 Autres

| Entreprise | Composant | Windows |
|---|---|---|
| GIE-SV | GALSS | 3.45.01 |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

# 4 MISES A JOUR DU PRODUIT

## 4.1 Description

Cette version succède à la version 5.2.6.

## 4.2 Récapitulatif

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

| Type | N° | Composant | Descriptif | Depuis |
|---|---|---|---|---|
| **E** | **4700** | **CCM** | Mise à jour du logo ANS sur le "à Propos" du CCM | 5.2.7<br>21/07/2026 |
| **C** | **4587** | **Installeur MSI** | Non désactivation du Minidriver CPS4 en BdR par l'installeur Cryptolib. | |
| **E** | **4586** | **CCM<br>Librairie PKCS#11** | Adaptation pour l'applet FIDO de la CPS4 | |
| **C** | **4438** | **Librairie PKCS#11** | Bug d'affichage sur le caractère copyright | |
| **E** | **4290** | **Librairie PKCS#11** | Cohabitation CPS4 et VPN SSA | |
| **C** | **4096** | **Librairie PKCS#11** | Possible crash d'une application utilisant la librairie PKCS#11 lors du retrait d'une carte CPS | 5.2.6<br>09/10/2025 |
| **C** | **4037** | **Librairie PKCS#11** | Blocage de l'appel à C_GetSlotList lorsqu'un slot est pris en exclusivité | |
| **C** | **3936** | **Librairie PKCS#11** | Blocage aléatoire sur Mac ARM avec CPS R4V4 | |
| **C** | **3667** | **Installeur MSI** | Non désactivation du Minidriver CPS4 en BdR par l'installeur Cryptolib. | 5.2.5<br>11/04/2025 |
| **C** | **1752** | **Librairie PKC#11<br>CPS3** | Echec d'une signature avec la clé d'authent avec une CPS4 : Logical channel not supported | 5.2.4<br>19/02/2025 |
| **C** | **1746** | **Librairie PKC#11<br>CPS3** | Potentielles fuites mémoire dans la librairie PKCS#11 | 5.2.3<br>24/01/2025 |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

| Type | N° | Composant | Descriptif | Depuis |
|---|---|---|---|---|
| C | 1743 | Librairie PKC#11 CPS3 | Erreur de signature RSA_PKCS avec la clé d'authentification lorsque la longueur demandée est supérieure à 256 | |
| C | 1722 | Librairie PKC#11 CPS3 | Correction sur la reprise des traitements Cryptolib suite à l'erreur statut carte 69 85 sur la CPS4 | 5.2.2 21/08/2024 |
| E | 1718 | Installeur MSI | Entrée T=0 à ajouter en BdR pour la CPS4 | 5.2.1 24/06/2024 |
| C | 1717 | Installeur MSI | DLLs CSP et P11 non supprimées par la désinstallation | |
| E | 1716 | Librairie PKC#11 CPS3 | Implémenter le chiffrement et remonter le flag CKF_ENCRYPT | |
| E | 1714 | Librairie PKC#11 CPS3 | Librairie PKCS#11CPS3 compatible CPS3/CPS4. | 5.2.0 30/05/2024 |
| E | 1713 | Installeur MSI | Réactiver la surveillance automatique des lecteurs par défaut dans le CCM | |
| E | 1712 | Librairie PKC#11 CPS3 | Exposé des labels PKCS11 pour les données de situation du volet CPS2TER (1 à 16 fichiers) | |


*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

# 5 PROBLEMES IDENTIFIES, CONSEILS ET PALLIATIFS

## 5.1 Note concernant les patchs FIDO2

Cette note est destinée aux structures utilisant à la fois des clés de sécurité FIDO2 et des cartes CPx, en particulier les officines utilisant des clés FIDO2 pour l'ouverture de sessions itinérantes avec Pro Santé Connect.

L'installation d'une Cryptolib CPS v5.2.7 pour Windows apporte 4 patchs FIDO permettant de résoudre d'éventuels problèmes de cohabitation pouvant apparaitre dans ce cas de figure.

Il existe un fichier *.reg* pour activer/désactiver chaque patch individuellement. Suite à l'installation d'une version de la Cryptolib CPS supérieure ou égale à 5.2.7, la note technique détaillée *note_technique_fido.md* ainsi que les fichiers *activation_fido_pX.reg* et *desactivation_fido_pX.reg*, sont disponibles dans le dossier ***C:\Program Files\santesocial\CPS\Patch_Fido***

Le tableau ci-dessous résume de manière synthétique dans quels cas et comment appliquer ces patchs. Les chapitres suivants détaillent le fonctionnement de chaque patch.

### 5.1.1 Cas d'usage et mode d'activation

| Patch | Problème rencontré | Cas d'usage et configurations concernées | Activé par défaut | Mode d'activation |
|---|---|---|---|---|
| P1 | Echec de l'utilisation d'une carte CPS4 en tant que clé FIDO2. | ➔ Carte CPS4 utilisée comme clé FIDO2. | NON | ➔ lancer *activation_fido_p1.reg* |
| P2 | Blocage des fonctionnalités métier des cartes CPx et Vitale lorsqu'une clé FIDO2 avec ATR est utilisée en parallèle. | ➔ Clé FIDO2 avec ATR (format badge NFC, carte à puce, ou clé USB intégrant un lecteur CCID virtuel), utilisée en parallèle des cartes CPx et Vitale. | NON | ➔ lancer *activation_fido_p1.reg*<br>➔ ajouter l'ATR de la clé FIDO2 dans *activation_fido_p2.reg*<br>➔ lancer *activation_fido_p2.reg*<br>➔ quitter CCM<br>➔ relancer CCM en mode Admin |
| P3 | Echec de lecture d'une carte CPS4 en parallèle de l'utilisation d'une clé FIDO2 pour l'accès à un VPN. | ➔ Cas d'usage et configuration spécifiques au SSA. | OUI | ➔ aucune action requise : patch P3 activé par défaut suite à l'installation de la Cryptolib CPS |
| P4 | Blocage des fonctionnalités métier des cartes CPx après une sortie de veille ou un déverrouillage de la session Windows. | ➔ Cartes CPx et clés FIDO2 utilisées en parallèle comme moyens d'authentifications. | NON | ➔ lancer *activation_fido_p1.reg*<br>➔ conserver P3 activé (par défaut)<br>➔ lancer *activation_fido_p4.reg* |



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*

### 5.1.2 Patch P1

Les modifications apportées par le patch P1 consistent à laisser le canal 01 ouvert uniquement si cela est nécessaire, afin de laisser les opérations FIDO prendre la main sur le canal 0, et à ajouter un délai à la propagation de certificats.

Ce patch a pour but de permettre à la carte CPS V4 d'être utilisée sur un même poste à la fois pour l'authentification FIDO et pour les opérations métier.

Pour activer le patch, double-cliquer sur *activation_fido_p1.reg*. Pour désactiver le patch, double-cliquer sur *desactivation_fido_p1.reg*.

### 5.1.3 Patch P2

Les modifications apportées par le patch P2 ont pour but d'empêcher Windows d'envoyer des commandes APDU SELECT FIDO en boucle***(*)*** aux cartes CPS V3/V4 (ou carte Vitale) lorsqu'une opération FIDO est initiée par un badge FIDO NFC présent sur un autre lecteur, ou une clé USB FIDO disposant d'un ATR***(**)***. Pour cela, CCM.exe prend une connexion SCardConnect en mode SCARD_SHARE_EXCLUSIVE sur les cartes à protéger dès qu'un badge FIDO amorce une opération FIDO, empêchant ainsi l'envoi de ces commandes.

Le patch P2 n'est fonctionnel que si le patch P1 est actif également. Pour son bon fonctionnement, le patch P2 nécessite que :

- L'ATR du ou des modèles de badges FIDO utilisées dans la structure soient ajoutés dans le paramètre "atr_badge_fido" du fichier *activation_fido_p2.reg*
- CCM.exe soit exécuté avec les droits administrateur.

Pour activer le patch, double-cliquer sur *activation_fido_p2.reg*. Pour désactiver le patch, double-cliquer sur *desactivation_fido_p2.reg*.

***(*)*** *Un ticket d'incident a été ouvert auprès de Microsoft concernant ce comportement inattendu.*
***(**)*** *L'ATR d'un modèle de badge FIDO2 peut être disponible sur le site du fabricant, ou consulté via la commande Windows « certutil -SCInfo ». Si vous utilisez une clé FIDO2 compatible Pro Santé Connect, le fichier d'activation contenant la liste des ATR de ces clés est disponible ici (fichier .txt à renommer en .reg).*

### 5.1.4 Patch P3

Les modifications apportées par le patch P3 ont pour but de resélectionner le canal 01 de la carte s'il était sur le canal 0, afin de rétablir ce canal pour les opérations métier.

Pour activer le patch, double-cliquer sur *activation_fido_p3.reg*. Pour désactiver le patch, double-cliquer sur *desactivation_fido_p3.reg*.

### 5.1.5 Patch P4

Les modifications apportées par le patch P4 ont pour but de resélectionner l'application CPS2TER de la carte au lieu de FIDO.

Lors d'une sortie de veille, Windows Hello envoie une commande APDU SELECT FIDO sur les cartes CPS V4. Cette commande sélectionne l'application FIDO au lieu de CPS2TER. Le patch P4 permet donc de resélectionner CPS2TER afin que les opérations métier puissent continuer à fonctionner.

Dix secondes après une sortie de veille, CCM.exe essayera de resélectionner CPS2TER après un SELECT FIDO si le patch est actif.

Le patch P4 n'est fonctionnel que si le patch P1 et P3 sont actifs également.

Pour activer le patch, double-cliquer sur *activation_fido_p4.reg*. Pour désactiver le patch, double-cliquer sur *desactivation_fido_p4.reg*.



*Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.*