RECOMMANDATIONS POUR UNE UTILISATION SÉCURISÉE DE CRYHOD

GUIDE ANSSI

ANSSI-BP-037
15/05/2017

PUBLIC VISÉ :

Développeur **Administrateur** **RSSI** **DSI** Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations pour une utilisation sécurisée de Cryhod** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	12/05/2017	Version initiale
1.1	15/05/2017	Correction mineure R22

Table des matières

1
Préambule

1.1 Le produit

Cryhod est un outil de chiffrement édité par la société *Prim'X*. Il permet de protéger en confidentialité les données présentes sur un support de stockage, en chiffrant l'ensemble du support ou certaines de ses partitions. Le produit protège principalement l'utilisateur du vol de son disque dur. Il est donc particulièrement adapté à la protection des données sur les postes nomades. L'utilisateur doit s'authentifier lors du démarrage de l'ordinateur pour pouvoir démarrer le système d'exploitation et accéder à ses données. Une fois la partition déverrouillée, le chiffrement des données est transparent pour l'utilisateur.

Le produit peut également être employé pour augmenter le niveau de sécurité de postes de travail contre la fuite de données. Il peut aisément se déployer sur un parc informatique en environnement Active Directory, sa configuration pouvant s'effectuer par le mécanisme de GPO.

1.2 Qualification du produit

La version 2.0 build 200 de *Cryhod* a été certifiée [CCB200] et qualifiée par l'ANSSI au niveau standard le 25 août 2011 [QSB200] pour la protection d'informations marquées :

- Diffusion Restreinte ;
- Restreint OTAN ;
- Restreint UE ;
- EUROCOR Diffusion Restreinte.

La version 2.0 buid 234 a également fait l'objet d'un rapport de maintenance [CCB234]. Les évolutions de *Cryhod* depuis la version qualifiée sont disponibles sur le site de l'éditeur, après authentification de l'utilisateur. Le produit analysé pour élaborer ce document est *Cryhod* version 3.0. Il est disponible sur le site de l'éditeur et est, à la date de publication de ce document, en phase de qualification par l'ANSSI.

Information

Au delà des recommandations contenues dans le présent document, l'agrément DR en cours d'instruction par l'ANSSI fixera l'ensemble des conditions d'utilisation de *Cryhod* pour la protection d'informations marquées « Diffusion Restreinte ».

1.3 Objectifs du document

Ce document fournit des recommandations pour un déploiement et une utilisation sécurisés du produit *Cryhod* sous Windows 7 et Windows 10. Il vient en complément des documents fournis par *Prim'X* afin d'approfondir l'aspect sécurité.

Il s'applique aux systèmes d'information sur lesquels *Cryhod* sera installé et s'adresse :

- aux équipes des SI qui devront mettre en place les recommandations ;
- aux membres de la DSI qui participeront au déploiement du produit, à son support auprès des utilisateurs et à son administration ;
- aux RSSI à qui reviennent les choix des mesures de sécurité, les modalités de leur mise en œuvre, ainsi que la gestion d'une éventuelle IGC.

Certaines recommandations de ce document peuvent également être transmises aux utilisateurs finaux. Le document aborde les problématiques de protection de l'environnement d'exécution du logiciel (section 3), la gestion des clés d'accès (section 4), les bonnes pratiques d'utilisation (section 5) ainsi que la configuration des politiques du logiciel (section 6).

2
Fonctionnement de Cryhod

2.1 Fonctionnement général

Cryhod permet de chiffrer les supports de stockage ou les partitions des postes de travail selon une politique de chiffrement définie. Le chiffrement et le déchiffrement sont effectués à la volée, de façon transparente pour les utilisateurs. *Cryhod* installe un micro-noyau, qui est chargé par le BIOS (ou l'UEFI) avant l'amorçage du système d'exploitation. Ce micro-noyau gère l'authentification de l'utilisateur et se charge ensuite de poursuivre le démarrage standard du système.

L'utilisateur peut s'authentifier à l'aide de différents moyens :

- un mot de passe ;
- un fichier contenant une clé privée (PFX/PKCS#12) ;
- une carte à puce ou jeton USB (PKCS#11) ;
- un conteneur Windows (CSP) (sous conditions).

La clé fournie par l'utilisateur (ou la clé dérivée de son mot de passe) est utilisée pour déverrouiller la clé de chiffrement du support de stockage. Lorsque cette clé est perdue, des mécanismes de récupération permettent à l'utilisateur de continuer à avoir accès à ses données. Toutes les opérations de gestion des accès et de chiffrement initial des partitions s'effectuent dans le « Centre de chiffrement ».

Les différents profils d'utilisateur du produit sont :

- l'*utilisateur standard*, qui est l'utilisateur du poste de travail ;
- l'*administrateur*, qui définit les accès et les politiques de chiffrement ;
- l'*opérateur de recouvrement*, qui intervient lorsque l'utilisateur a perdu son accès.

2.2 Configuration

Cryhod est paramétrable selon un ensemble de règles qui définissent son comportement. Ces politiques sont décrites dans le *Guide d'utilisation* et listées sous forme de points à vérifier dans le *Memento policies* fournis par l'éditeur. Ces documents sont accessibles sur le site Internet de *Prim'X* après authentification.

Selon le cas d'usage et l'environnement dans lequel se trouve le poste de travail, la configuration des politiques appliquées à ce poste peut s'effectuer de plusieurs manières.

2.2.1 Poste dans un environnement Active Directory

Dans un environnement Active Directory, les politiques peuvent être administrées depuis un contrôleur de domaine sur lequel ont été ajoutés les modèles d'administration *Cryhod* fournis par l'éditeur. Ces modèles peuvent être récupérés en installant *Cryhod* sur un poste et en parcourant le dossier `C:\Windows\PolicyDefinitions`. Les fichiers à récupérer sont `Primx.amdx` et `Cryhod.admx` et les fichiers de langue `Primx.amdl` et `Cryhod.adml` associés.

Une fois ces politiques configurées, elles pourront être déployées via les stratégies de groupe (GPO) sur les machines du parc.

Information

La note technique [AD] éditée par l'ANSSI détaille les recommandations de sécurité à suivre lors de l'utilisation de GPO dans un environnement Active Directory.

2.2.2 Poste isolé

Sur un poste isolé, l'administration des politiques s'effectue au travers de la console « Éditeur de stratégie de groupe locale » (`gpedit.msc`), elles seront directement appliquées au poste.

Cryhod version 3.0 apporte un nouveau mode de configuration des politiques, via un fichier XML. Le chemin d'accès à ce fichier XML est néanmoins à configurer dans une politique (P070) via la console « Éditeur de stratégie de groupe locale ».

2.3 Limites d'utilisation

Attention

Cryhod protège le poste de travail de menaces telles que le vol du poste ou du support de stockage. Certaines techniques malveillantes, telles que le piégeage, peuvent néanmoins contourner les mécanismes de sécurité mis en place.

Un attaquant ayant corrompu le système d'exploitation de l'utilisateur pourra accéder aux données protégées dès le déverrouillage du poste. La section suivante détaille quelques contre-mesures.

Attention

Cryhod ne protège pas les données une fois que l'utilisateur s'est authentifié sur l'écran de pré-amorçage.

3
Sécurité de l'environnement d'exécution de Cryhod

Cryhod est un logiciel installé sur le poste de travail de l'utilisateur. La sécurité qu'il apporte est donc dépendante de son environnement d'exécution, et notamment du niveau de protection :

- des informations sensibles et cryptographiques transitant en mémoire (clés privées, mots de passe, fichiers déchiffrés) ;
- des exécutables du logiciel (qu'il faut protéger en intégrité) ;
- du système d'exploitation sur lequel il s'exécute.

Il est donc primordial de sécuriser l'environnement physique et logiciel d'exécution de *Cryhod*.

3.1 Protection physique

R1

Protection physique du poste de travail

Il est recommandé de mettre en place des mesures assurant la protection physique des postes de travail lorsqu'ils ne sont pas sous la surveillance de leur utilisateur.

En effet, il est particulièrement difficile, voire impossible, de garantir l'intégrité d'un poste informatique si un attaquant a pu avoir un accès physique à la machine. Il lui est possible de piéger physiquement le matériel, ou d'installer des programmes malveillants dans les secteurs de démarrage. L'utilisation de TPM (Trusted Module Platform) ou Secure Boot, sous Windows, permet d'éviter une partie de ces attaques, sans garantie absolue.

Dans le cadre de la mobilité, l'utilisateur devra porter d'autant plus d'attention à son poste. Un poste suspecté d'avoir été volé, ou même accédé pendant un court instant, devra être complètement réinstallé.

3.2 Protection logicielle

3.2.1 Maîtrise du poste utilisateur

Les utilisateurs ne doivent pas pouvoir modifier les paramètres de configuration de *Cryhod*. Ils risqueraient, volontairement ou non, de dégrader le niveau de sécurité. Seuls les administrateurs

doivent être autorisés à le faire.

R2

Maitrise du poste de travail

Cryhod doit être installé sur un poste maîtrisé dont l'utilisateur n'est pas administrateur.

R3

Protection d'un poste de travail de niveau Diffusion Restreinte

Des moyens de protection doivent être mis en place afin de protéger le poste de travail des réseaux non sécurisés (Internet notamment).

3.2.2 Garantie de l'intégrité du code exécutable

Les fichiers exécutables et les bibliothèques fournis par *Prim'X* sont signés numériquement. Ceci permet de vérifier que le code des exécutables et des bibliothèques associées n'a pas été modifié par un attaquant. L'autorité de certification choisie par *Prim'X* est Verisign.

La signature du code n'est cependant pas vérifiée lors de l'exécution du programme mais uniquement lors de l'inspection manuelle de la validité de la signature. En effet, la modification du contenu binaire ne déclenche pas d'alerte lors de l'utilisation de l'outil dans la configuration par défaut de Windows. Une solution envisageable, lorsque cela est possible dans le système d'information hôte, est de passer par les « Politiques de restriction logicielle » de Windows afin de forcer cette vérification. La note technique [APPLOCKER-2.0] détaille ce mécanisme.

R4

Activation des politiques de restriction logicielle

La mise en œuvre de la protection de l'intégrité des exécutables par les politiques de restriction logicielle Windows est recommandée dès lors que cette mesure est déjà en place dans le SI hôte.

4
Gestion des clés d'accès

Pour chiffrer et déchiffrer les données, *Cryhod* utilise un algorithme symétrique, car la cryptographie symétrique montre des performances bien plus élevées que la cryptographie asymétrique. La clé symétrique utilisée est chiffrée par la « clé d'accès » de l'utilisateur, qui est asymétrique dans le cas de l'utilisation de certificats ou symétrique dans le cas où elle est dérivée du mot de passe défini par l'utilisateur ou l'administrateur.

4.1 Choix des types d'accès

Cryhod propose quatre moyens d'authentification, comme décrit au paragraphe 2.1. L'utilisation de certificats issus d'une IGC présente plusieurs avantages. Cela augmente le niveau de sécurité, en particulier car il faut posséder deux informations (la clé privée et le mot de passe pour déverrouiller la clé privée). Du point de vue opérationnel, lorsqu'un annuaire (Active Directory par exemple) est déjà utilisé dans le système d'information, il est plus aisé de mettre en place l'authentification par certificat que par mot de passe. *Cryhod* est en effet capable d'utiliser les certificats associés aux utilisateurs dans l'annuaire.

De plus, les fonctions de séquestre et de recouvrement peuvent être portées par l'IGC et non par un opérateur de recouvrement dédié à *Cryhod*.

R5

Choix des types d'accès

Dès lors que des utilisateurs disposent de certificats de chiffrement issus d'une IGC de confiance, leur usage doit être préféré à celui du mot de passe.

Les certificats doivent respecter les attributs définis au paragraphe 6.1.1.

L'utilisation d'un support cryptographique matériel (carte à puce, token USB) augmente le niveau de sécurité de manière significative. Outre le fait d'apporter un facteur d'authentification supplémentaire, il protège la clé privée en confidentialité et en intégrité.

R6

Utilisation de supports cryptographiques

Privilégier le stockage de la clé privée sur un support cryptographique matériel (carte à puce, token PKCS#11…).

Les bonnes pratiques de configuration des différents types d'accès sont détaillées dans le paragraphe 6.1.

4.2 Accès par clés asymétriques

Cryhod propose d'authentifier l'utilisateur par certificat, qu'il soit logiciel (conteneur PKCS#12, CSP) ou embarqué dans un matériel cryptographique (PKCS#11). Dans les deux cas, l'accès à la clé privée associée au certificat doit être protégée. Cette clé ne doit pas être accessible en clair sur le disque du poste de travail, un accès au poste déverrouillé suffirait alors à s'authentifier à l'avenir sur le poste. Par exemple, le conteneur PKCS#12 doit être protégé par un mot de passe. De même, une clé embarquée sur une carte à puce doit être protégée par un code PIN et non exportable. La note technique [MDP] fournit des éléments pour définir des mots de passe robustes.

R7

Protection de la clé privée personnelle dans le cas d'un fichier

La clé privée ne doit jamais être stockée en clair et doit être protégée par un mot de passe robuste. Ce mot de passe doit être choisi et uniquement connu par le propriétaire de la clé.

R8

Protection de la clé privée personnelle dans le cas d'une carte à puce

La clé privée stockée sur la carte à puce doit être protégée par un code PIN et ne pas être exportable. Le code PIN doit être choisi et uniquement connu par le propriétaire de la clé.

Les différentes clés utilisées doivent être régulièrement renouvelées, afin de limiter l'impact d'une compromission de l'une d'entre elles ou d'attaques cryptographiques.

R9

Gestion de la cryptopériode des clés

Il est recommandé que la cryptopériode (durée de vie) des clés ne dépasse pas 3 ans.

Le « Centre de chiffrement » propose une interface pour changer le certificat utilisé pour accéder au disque. Seule la clé d'accès est changée, la clé symétrique chiffrant effectivement les données reste identique.

R10

Transchiffrement du disque

Lors du changement de certificat suite à son expiration, il est recommandé de transchiffrer les partitions afin de renouveler la clé de chiffrement des données.

Pour éviter l'interception des informations d'authentification, les conteneurs logiciels ou matériels cryptographiques et les mots de passe associés ne doivent pas transiter par les mêmes canaux de communication. Ainsi, si un attaquant est capable d'intercepter les informations transitant sur un canal, il ne pourra pas utiliser les informations volées en l'état.

R11

Distribution des clés et des mots de passe

Il est recommandé de diffuser les conteneurs logiciels ou matériels cryptographiques et les mots de passe associés par des canaux distincts.

4.3 Accès par mots de passe

Pour les organisations ne possédant pas d'IGC, *Cryhod* propose également d'authentifier l'utilisateur à l'aide d'un mot de passe. De la même façon qu'une clé, le mot de passe doit être uniquement connu de l'utilisateur du poste de travail.

R12

Protection des mots de passe

Le mot de passe utilisé pour authentifier l'utilisateur sous *Cryhod*

- ne doit jamais être stocké en clair ni écrit (fichier mémo, post-it…) ;
- doit être défini et uniquement connu par son propriétaire ;
- ne doit pas être utilisé pour d'autres services ou applications.

Le paragraphe 6.1.2 traite des politiques de complexité des mots de passe.

5
Bonnes pratiques d'utilisation

5.1 Choix des partitions à chiffrer

L'administrateur de la solution *Cryhod* doit implémenter une politique de chiffrement. Cette politique définit les supports de stockage et les partitions à chiffrer ainsi que le caractère obligatoire ou non de ce chiffrement.

R13

Choix des partitions à chiffrer

Il est recommandé de chiffrer l'intégralité des supports de stockage du poste de travail, afin d'éviter toute exposition de contenu sensible.

5.2 Recouvrement

Lorsque l'utilisateur a perdu son mot de passe ou son jeton d'authentification, il existe plusieurs moyens pour qu'il puisse néanmoins utiliser son poste de travail :

- le séquestre de sa clé d'accès, dans le cas d'un accès par certificat ;
- la création d'accès obligatoires de recouvrement.

5.2.1 Séquestre des clés

Lorsque le type d'accès choisi est le certificat, les clés privées des utilisateurs doivent être séquestrées. Un opérateur de séquestre peut alors récupérer la clé d'accès de l'utilisateur.

Le séquestre offre de meilleures garanties de sécurité dès lors qu'il est déconnecté du réseau et se contente de fournir à nouveau la clé de l'utilisateur en cas de perte de la carte. À l'inverse, un accès de recouvrement fournit un accès unique à l'ensemble des informations chiffrées par l'entité. La perte ou la fuite de cet accès unique de recouvrement vers un attaquant donne accès à l'ensemble des données protégées.

R14

Séquestre des clés

Lorsqu'un accès par certificats est utilisé, il est recommandé de privilégier le séquestre des clés plutôt qu'un accès obligatoire aux partitions.

5.2.2 Procédure de secours à distance

Lorsque le type d'accès choisi est le mot de passe ou qu'un séquestre des clés est impossible, il est possible pour un opérateur de recouvrement de débloquer l'accès d'un utilisateur. Un accès de re-

couvrement doit avoir été créé au préalable sur les partitions à déchiffrer. Il faudra que l'opérateur déverrouille le poste et aide l'utilisateur à changer son mot de passe ou son certificat.

Pour éviter de faire déplacer physiquement un opérateur de recouvrement, il est possible d'utiliser la procédure de secours distante. L'utilisateur affiche la fenêtre de secours lors de l'écran d'authentification au pré-démarrage en appuyant sur la touche F7. Il doit ensuite contacter le *helpdesk* de son organisation, dont les coordonnées seront affichées à l'écran, et lui communiquer le numéro de ticket généré par *Cryhod*. Le *helpdesk* utilise un outil fourni par *Prim'X* (`cyred.exe`) et dispose de la cartographie de chiffrement du poste (voir paragraphe 6.2). Il transmet au choix à l'utilisateur :

- un fichier de secours ;
- un laissez-passer temporaire ;
- un mot de passe de secours personnel.

Le fichier de secours est un fichier à présenter sur un support USB lors de l'authentification pré-démarrage, accompagné d'un code de déblocage. Le laissez-passer temporaire est un code de déverrouillage du poste qui n'est valable que pour un certain nombre de démarrages et pour une période donnée (configurables dans une politique). Ce laissez-passer est désactivé lorsque l'utilisateur clôt le ticket de dépannage. Le mot de passe de secours est un mot de passe robuste défini automatiquement pour chaque partition chiffrée.

Les politiques de *Cryhod* doivent être appliquées sur les machines du *helpdesk* qui utilisent l'outil `cyred.exe`, afin qu'elles possèdent une configuration compatible avec les clients, notamment au niveau des algorithmes cryptographiques.

R15

Procédure de secours distante

Lors de l'appel téléphonique au *helpdesk*, il est recommandé de s'assurer de l'identité de l'utilisateur par une procédure offrant de véritables garanties de l'identité de l'appelant et de privilégier l'accès temporaire.
Il est également fortement recommandé de ne pas utiliser le mécanisme de laissez-passer temporaire auprès d'utilisateurs qui ne seraient pas de confiance.

Ce choix est dicté par des raisons organisationnelles (aucun fichier à transmettre à l'utilisateur) et des raisons de sécurité (l'utilisateur n'aura qu'un mot de passe temporaire et non pas un fichier ou mot de passe permettant de déverrouiller son disque jusqu'à ce que l'administrateur le change).

Attention

Il faut également noter que le caractère temporaire de l'accès vise à inciter l'utilisateur à utiliser ses accès personnels plutôt que ceux de secours et ne garantissent pas qu'un utilisateur malveillant ayant utilisé un accès temporaire ne puisse, grâce à celui-ci, déchiffrer des données par la suite.

6
Configuration des politiques

Les différents paramètres de *Cryhod* (y compris de sécurité) sont définis dans des politiques, configurables par la console Windows `gpedit.msc` ou par fichier XML.

6.1 Gestion des accès

Cryhod supporte quatre mécanismes d'authentification différents. Les politiques suivantes permettent d'interdire certains de ces types d'accès aux utilisateurs :

- P102 : interdire les accès par mot de passe pour déverrouiller les disques ;
- P103 : interdire les fichiers de clés PKCS#12 pour déverrouiller les disques ;
- P104 : interdire les cartes ou jetons PKCS#11 pour déverrouiller les disques ;
- P105 : interdire les fournisseurs CSP pour déverrouiller les disques.

Activer une de ces politiques bloquera le moyen d'authentification associé, la désactiver autorisera ce moyen.

R16

Limitation des types d'accès

Il est recommandé d'interdire les types d'accès non utilisés dans le scénario de déploiement retenu.

Attention

L'activation simultanée des quatre politiques bloquera l'ensemble des types d'accès et donc l'accès au poste de travail. Il convient de s'assurer qu'au moins une de ces politiques est toujours désactivée.

La politique P802 définit le comportement de *Cryhod* relatif à la réutilisation des clés d'accès fournies au démarrage. Cette fonctionnalité permet de fournir automatiquement le mot de passe ou la clé privée de l'utilisateur aux programmes *Prim'X* installés sur le poste (*Cryhod*, *ZoneCentral*) après authentification. Cette pratique présente plusieurs risques. Le premier vient du fait que la clé d'accès sera présente dans la mémoire de l'ordinateur pendant quelques minutes. Le second se présente sur les postes partagés entre plusieurs utilisateurs (ou intégrés dans un AD) : la clé sera disponible pour toute session Windows, pas seulement celle du propriétaire de la clé. Un autre utilisateur qui ouvrira sa session sur le même poste pourra alors avoir accès à des zones *ZoneCentral* auxquelles il ne devrait pas.

R17

Absence de réutilisation des clés fournies au démarrage

Il est recommandé d'activer la politique P802 et de choisir l'option « ne pas réutiliser les clés d'accès du démarrage ».

Information

Lorsque le SSO *Cryhod* (qui permet d'enregistrer l'identifiant et mot de passe de la session Windows) est utilisé et que la politique P802 est désactivée, *Cryhod* ne mettra pas automatiquement à jour le mot de passe de la session Windows renseigné dans l'écran d'authentification pré-démarrage. Cette opération devra être effectuée manuellement lors d'un changement de mot de passe de session Windows.

6.1.1 Accès par certificat

Les politiques P129, P140 à P143, P146 et P147 configurent les contrôles réalisés sur les certificats. Ces contrôles permettent de limiter le risque qu'un certificat illégitime ou volé soit utilisé dans *Cryhod*. Nous allons aborder ces politiques une à une.

La politique P129 configure la création de l'accès de l'utilisateur lorsque celui-ci utilise un certificat. Cette politique peut laisser l'utilisateur choisir un certificat, ou bien imposer que son certificat associé dans l'annuaire soit utilisé. Ce dernier choix simplifie la tâche de l'administrateur et de l'utilisateur.

R18

Choix du certificat

Lorsque les certificats utilisateurs sont publiés dans un annuaire, il est recommandé d'activer la politique P129 et de choisir la valeur « 2-annuaires(obligatoire) ».

La création d'un accès par certificat issu d'un annuaire nécessite une connexion à cet annuaire. La requête LDAP pour récupérer le certificat dans l'annuaire peut être configurée dans la politique P136.

R19

Configuration de l'annuaire

Renseigner la politique P136 selon la configuration de l'annuaire local.

Cryhod est capable de vérifier l'état de révocation d'un certificat en consultant la liste de révocation dont le chemin d'accès (HTTP ou LDAP) est renseigné dans l'extension `CRL Distribution Point` du certificat. La politique P140 contrôle l'activation de cette fonctionnalité dans le produit.

R20

Contrôle des listes de révocation

Il est recommandé de désactiver la politique P140, afin de vérifier l'état de révocation des certificats.

Dans le but de prévenir l'utilisation d'un certificat non autorisé, il est possible de restreindre les autorités de certification autorisées grâce à la politique P141. Si les certificats utilisés pour l'authentification dans *Cryhod* proviennent d'une IGC interne, seule la racine de cette IGC (ou une autorité de certification intermédiaire) doit être autorisée. Lorsqu'une autorité de certification intermédiaire est autorisée, il faut également autoriser toute la chaîne de certification au dessus de

cette autorité.

R21

Gestion des autorités racines

Il est recommandé d'activer la politique P141 et de limiter les racines autorisées à la liste des racines et autorités de certification intermédiaires qui émettent effectivement les certificats d'authentification *Cryhod*.

Par la politique P142, il est possible d'autoriser l'utilisation de certificats après leur date d'expiration pour la création de nouveaux accès, pendant un temps défini par la politique P143. Il reste toujours possible d'utiliser un certificat périmé pour obtenir un accès précédement créé.

R22

Création d'un accès à un certificat expiré

Il est recommandé de désactiver la politique P142, afin d'interdire la création d'un accès à un certificat expiré.

Par défaut, dès lors que l'accès d'un utilisateur est protégé par un certificat X.509, *Cryhod* requiert que l'extension `Key Usage` du certificat soit présente et contienne au moins la valeur `Key Encipherment`. L'activation de la politique P146 permet de désactiver cette vérification.

R23

Contrôle de l'usage de clé

Il est recommandé de ne pas activer la politique P146, afin de forcer la vérification de l'extension `Key Usage` du certificat.

6.1.2 Accès par mot de passe

Il convient de rappeler que l'usage des certificats doit être privilégié, comme précisé dans la partie 4.1. Toutefois, dans le cas de l'utilisation de mots de passe, les politiques P710 à P724 définissent des règles relatives à leur robustesse. La note technique [MDP] fournit des éléments pour mettre en place une politique de mots de passe robuste.

R24

Complexité des mots de passe

Il est recommandé d'utiliser les valeurs par défaut (à la date de rédaction de ce document : 10 caractères, dont 2 minuscules, 2 majuscules, 1 caractère spécial et 1 nombre) des politiques P712 à 720 et de régler le seuil d'acceptation du mot de passe (P710) à 100%.

6.2 Recouvrement

Comme décrit au paragraphe 5.2, plusieurs mécanismes de déverrouillage du poste de travail peuvent être utilisés lorsque l'utilisateur perd son moyen d'authentification.

Le mécanisme du séquestre des clés est à privilégier. Comme l'utilisateur obtiendra le recouvrement de ses clés par l'opérateur de recouvrement de l'IGC, un accès obligatoire sur chaque partition n'est pas nécessaire.

R25

Accès obligatoire et séquestre des clés

Lorsqu'un séquestre des clés est mis en place, il est recommandé de ne pas définir d'accès obligatoire. Le nom de la valeur de la politique P131 doit alors être `none` et la valeur doit être vide.

Si des procédures de secours à distance sont mises en œuvre, un « accès obligatoire » doit être automatiquement ajouté dans chaque partition. Le propriétaire de cet accès pourra alors déchiffrer toutes les partitions du parc sur lesquelles *Cryhod* est déployé. La politique P131 permet de configurer cet accès, défini par une liste d'accès (fichier `.zaf`) ou un certificat.

R26

Accès obligatoire et secours à distance

Lorsqu'un « accès obligatoire » est défini, le type d'accès doit être particulièrement robuste. Il est recommandé d'utiliser un certificat, de préférence stocké sur un support cryptographique matériel.

Afin de pouvoir aider un utilisateur, l'opérateur de recouvrement doit avoir accès à l'état de chiffrement (partitions chiffrées et accès) du poste à déverrouiller. Pour cela, *Cryhod* exporte un fichier (extension `.cymap`) représentant la cartographie de chiffrement du poste. La politique P821 permet de configurer l'emplacement où sera exporté ce fichier. Cet emplacement peut être un partage réseau, accessible en écriture par tous. Ce fichier est exporté à chaque opération de maintenance (premier chiffrement d'une partition, modification des accès) lorsque le poste est connecté à son système d'information. L'opérateur utilisera la dernière version présente sur le SI.

Comme exprimé au paragraphe 5.2.2, il est préférable d'utiliser le « laissez-passer temporaire » pour le secours à distance. La politique P264 configure ce choix. Lors de la configuration de la politique P264, il est possible de configurer également la politique P842 qui fixe la durée de vie et le nombre de démarrages autorisés avec un laissez-passer.

R27

Configuration des accès de secours

Il est recommandé d'activer la politique P264 et de sélectionner la valeur « laissez-passer temporaire uniquement ». Le ticket de dépannage doit être clos dès que possible afin d'empêcher l'accès à un potentiel attaquant qui aurait eu accès au laissez-passer temporaire. Il est recommandé pour la politique P842 de laisser les valeurs par défaut (`days=3;use=15`) ou de les durcir.

6.3 Protection des fichiers stratégiques

Les fichiers de cartographie sont utilisés par *Cryhod* pour stocker les informations relatives au chiffrement : les algorithmes utilisés, les clés de déchiffrement protégées par les clés d'accès au disque, les clés utilisées pour le recouvrement, etc. Ces fichiers sont stockés dans un ou plusieurs emplacements renseignés dans la politique P821.

De même, si le choix du mode de déploiement aboutit à l'utilisation de listes d'accès personnelles, celles-ci se présentent aussi sous la forme de fichiers. Bien que protégés, ces fichiers contiennent

des informations sensibles. De plus, pour des raisons fonctionnelles, ils sont stockés à de multiples emplacements définis dans les politiques P121 (emplacement de référence), P122 (emplacement de cache) et P127 (emplacement distant).

Dans le cas de postes nomades pouvant donc être volés ou perdus, il est important de conserver une copie de secours de ces fichiers essentiels dans le système d'information de l'entreprise. Les espaces réseaux partagés sont alors un emplacement tout indiqué pour cet usage. Il faudra cependant alors veiller à ce qu'un utilisateur ne puisse écrire et lire que ses propres fichiers, par des mécanismes de droits d'accès à définir selon la technologie de stockage utilisée. Dans le cas contraire, des scénarios d'attaque sont envisageables entre des utilisateurs légitimes du produit.

R28

Protection des fichiers stratégiques

Les fichiers de cartographie et les fichiers de listes d'accès, dont les emplacements sont renseignés dans les politiques P821, P121, P122 et P127 ne doivent être accessibles en écriture et en lecture qu'à leur propriétaire et aux administrateurs de sécurité afin d'éviter des attaques par des utilisateurs malveillants.

6.4 Politique de chiffrement

La politique P820 permet de définir la politique de chiffrement du poste, c'est-à-dire quelles partitions seront chiffrées et quel sera le pouvoir de décision de l'utilisateur.

R29

Politique de chiffrement

Il est recommandé d'inclure les mots clés `user=0;auto=1` dans les règles de la politique P820, afin de chiffrer systématiquement les partitions sans modification possible par l'utilisateur.

La mise en veille du poste peut être trompeuse : l'utilisateur peut croire que son poste est éteint ou en veille prolongée alors qu'il n'est pas verrouillé par *Cryhod* et que la mémoire vive n'est pas chiffrée. Dans le cas de la mise en veille prolongée, le contenu de la mémoire vive est écrit sur le disque et donc chiffré par *Cryhod*. Par défault, *Cryhod* désactive la mise en veille simple du poste et n'autorise que la mise en veille prolongée. Lors du réveil, l'utilisateur doit fournir ses éléments d'authentification. La politique P801 permet d'activer la mise en veille simple.

R30

Gestion de la mise en veille

Il est recommandé de désactiver la politique P801, afin d'interdire la mise en veille simple.

6.5 Cryptographie

La configuration des options cryptographiques est effectuée par les politiques P290 à P383. Cette configuration doit se faire en accord avec le Référentiel général de sécurité [RGS]. La politique

P292 configure l'algorithme de hachage utilisé par *Cryhod*. Cet algorithme intervient notamment durant la dérivation de clés à partir du mot de passe.

R31

Conformité de l'algorithme de hachage

Il est recommandé d'activer la politique P292 et de choisir la valeur SHA-256.

La politique P383 configure le mode de chiffrement mis en œuvre par RSA. La version 1.5 de PKCS#1 présente des vulnérabilités connues depuis 1998 [DB98]. Néanmoins, tous les logiciels de chiffrement et matériels cryptographiques ne supportent pas encore les version 2.1 ou 2.2.

R32

Utilisation de PKCS#1 v2.2

Il est recommandé d'utiliser un matériel cryptographique supportant le standard PKCS#1 v2.2, d'activer la politique P383 et de sélectionner la valeur 2 (PKCS#1 v2.2 avec utilisation de SHA-256).

6.6 Journaux d'événements

Par défaut, *Cryhod* consigne ses évènements dans le journal d'évènements du système (section *journaux des applications et des services*). Les politiques P303 et P304 activent ou désactivent la journalisation des opérations d'administration réussies ou échouées.

R33

Évènements journalisés

Il est recommandé au minimum de journaliser les opérations d'administration en échec.

La politique P301 permet d'indiquer une machine Windows vers laquelle ces journaux d'événements seront exportés.

R34

Export des journaux

Lorsque l'export des journaux d'évènements Windows n'est pas mis en place, il est recommandé d'exporter les journaux d'événements *Cryhod* vers un collecteur de journaux Windows.

La note technique [LOGS] présente les bonnes pratiques permettant de bâtir une architecture de gestion de journaux.

6.7 Signature des politiques

Afin de prévenir la modification des politiques par un utilisateur malveillant, celles-ci peuvent être signées, et *Cryhod* configuré pour n'accepter que les politiques signées.

R35

Signature des politiques

Il est recommandé de signer les politiques selon le guide *Mise en œuvre de la signature des politiques* fourni par *Prim'X*.

Le document de mise en œuvre de la signature des politiques est également disponible sur le site de l'éditeur, après authentification.

Glossaire

AD	*Active Directory*
AES	*Advanced Encryption Standard*
ANSSI	Agence nationale de la sécurité des systèmes d'information
Build	Sous-version du logiciel, permet de suivre les évolutions du logiciel entre deux changements de version mineure
DSI	Direction des systèmes d'information
EUROCOR DR	Marquage d'une information de niveau diffusion restreinte au sein du corps d'armée *Eurocorps*
GPO	*Global Policy Object* (stratégies de groupe)
IGC	Infrastructure de gestion de clés
Information DR	Information marquée « diffusion restreinte »
OID	*Object IDentifier*, identifiant universel normalisé
OTAN	Organisation du traité de l'atlantique nord
PSSI	Politique de sécurité des systèmes d'information
RGS	Référentiel général de sécurité
RSOP	*Resultant Set Of Policy*, un outil de visualisation des GPO appliquées sur une cible
RSSI	Responsable de la sécurité des systèmes d'information
SHA256, SHA1	Algorithmes de hachage
SI	Système d'information
SSO	*Single Sign-On*
TPM	*Trusted Platform Module*
UE	Union Européenne
X.509	Norme de certificat électronique définie dans la RFC5280

Liste des recommandations

Bibliographie

[CCB200] *Cryhod version 2.0 build 200*.
Rapport de certification ANSSI-CC-2011/20, ANSSI, juillet 2011.
https://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC_2011-20fr.pdf.

[CCB234] *Cryhod version 2.0 build 234*.
Rapport de maintenance ANSSI-CC-2011/20-M01, ANSSI, juillet 2013.
https://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC_2011-20-M01fr.pdf.

[MDP] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[LOGS] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[APPLOCKER-2.0] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP, ANSSI, janvier 2017.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

[AD] *Recommandations de sécurité relatives à Active Directory*.
Note technique DAT-NT-017/ANSSI/SDE/NP, ANSSI, septembre 2014.
https://www.ssi.gouv.fr/Active-Directory.

[QSB200] *Cryhod version 2.0 build 200*.
Rapport 2177/ANSSI/SR/RGL, ANSSI, août 2011.
https://www.ssi.gouv.fr/uploads/IMG/qualification/2011-08-25_2177_anssi_sr_rgl.pdf.

[RGS] *RGS : Référentiel Général de Sécurité*.
Referentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[DB98] Daniel Bleichenbacher.
Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS1.
In *LNCS 1462*, pages 1–12. Springer-Verlag, 1998.
http://archiv.infsec.ethz.ch/education/fs08/secsem/Bleichenbacher98.pdf.

ANSSI-BP-037
Version 1.1 - 15/05/2017

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE