

RECOMMANDATIONS POUR UNE UTILISATION SÉCURISÉE DE ZED !

GUIDE ANSSI

PUBLIC VISÉ :

Développeur

Administrateur

RSSI

DSI

Utilisateur



Informations



Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations pour une utilisation sécurisée de Zed!** ». Il est téléchargeable sur le site www.ssi.gouv.fr.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [ETALAB].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Ces recommandations n'ont pas de caractère normatif, elles 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	12/01/2016	Version initiale
1.1	14/11/2019	Modification mineure suite au passage de Zed! à la version 6.1

Table des matières

1	Préambule	4
1.1	Le produit	4
1.2	Qualification du produit	4
1.3	Objectifs du document	5
1.4	Cas d’usage étudié	5
1.5	Définition des menaces abordées	5
2	Fonctionnement de Zed	7
2.1	Présentation des accès sur <i>Zed</i>	7
2.2	Limites d’utilisation	7
3	Sécurité de l’environnement d’exécution de Zed	9
3.1	Protection physique	9
3.2	Protection logicielle	9
3.2.1	Maîtrise du poste utilisateur	10
3.2.2	Garantie de l’intégrité du code exécutable	10
3.2.3	Mise à jour	10
4	Gestion des clés d’accès	11
4.1	Accès par clés asymétriques (accès de type PKCS#12, PKCS#11 ou CSP)	11
4.2	Accès par mots de passe	11
4.3	Choix des types d’accès	12
5	Bonnes pratiques d’utilisation	13
5.1	Liste des accès	13
5.2	Utilisation des clés fonctionnelles	13
5.3	Intégrité et authenticité des données	14
6	Configuration des politiques	15
6.1	Modalités de la configuration de <i>Zed</i>	15
6.1.1	Environnement AD	15
6.1.2	Poste Linux	15
6.2	Contrôle des politiques	15
6.3	Restriction des types d’accès autorisés	16
6.3.1	Désactivation de l’accès de secours	16
6.4	Interaction avec l’infrastructure de gestion des clés	17
6.4.1	Accès obligatoires (P131 et P139)	17
6.4.2	Racines autorisées (P141)	17
6.4.3	Affectation des certificats	17
6.4.4	Dates de validité des certificats (P142, P143, P186 et P187)	18
6.4.5	Relaxer le contrôle d’usage (P146)	18
6.4.6	Utilisation des usages de clé étendus (P148)	18
6.4.7	Annuaire de recherche des certificats de correspondants	19
6.5	Affichage des noms de fichiers et des noms de dossiers au sein d’un conteneur (P233)	19
6.6	Contrôle des mots de passe	19

6.6.1	Complexité des mots de passe des utilisateurs (P730, P732-742)	19
6.6.2	Authentification unique par Windows (P110)	19
6.6.3	Activation du carnet de mots de passe (P750)	20
6.7	Algorithmes cryptographiques	20
6.7.1	Algorithme de chiffrement (P290, P291)	20
6.7.2	Algorithme de hachage (P292)	20
6.7.3	Dérivation des mots de passe (P290, P291, P293, P294 et P295)	21
6.7.4	Cartes et jetons PKCS#11 supportés et autorisés (P296)	21
6.7.5	Conteneurs v2 (P399)	21
6.7.6	PKCS#1 v2.2 (P383)	22
6.8	Correction de la CVE-2018-16518	22
7	Signature des politiques	23
	Liste des recommandations	24
	Bibliographie	25

1

Préambule

1.1 Le produit

Zed est un outil de chiffrement édité par la société *Prim'X*. Il permet de protéger des fichiers au sein de conteneurs à des fins d'archivage, d'échange par courriel sur des réseaux publics (Internet) ou par support physique (clé USB). Les données chiffrées ne sont alors accessibles qu'aux destinataires choisis par le créateur du conteneur. Elles sont hébergées dans un fichier utilisant l'extension *.zed*. Il est possible de chiffrer les données avec un mot de passe, des certificats, des cartes à puce et des jetons USB.

Le comportement des conteneurs est très semblable à celui d'une archive dans un environnement Windows. Le glisser-déposer ainsi que la modification des fichiers au sein de l'archive sont en effet possibles.

Zed utilise aussi une fonction de compression permettant de réduire la taille des données chiffrées.

1.2 Qualification du produit

La version 6.1 de *Zed* a été qualifiée au niveau standard en janvier 2019 [[RefAn1](#)][[RefPx8](#)][[RefAn2](#)]. Les versions 6.1 du build 2120 et 2121 avaient l'objet d'une certification et qualification en 2016 et 2018.

La fonction de création et consultation des conteneurs *Zed* est en cours de réagrément à ce jour pour la protection des informations jusqu'à un niveau Diffusion Restreinte, Restreint OTAN, ou Restreint UE.

Les évolutions de *Zed* depuis la version qualifiée sont renseignées dans les *Fix Notes* disponibles sur le site de *Prim'X* [[RefPx8](#)].

Le produit analysé pour élaborer ce document est *Zed* en version 6.1.

1.3 Objectifs du document

Ce document fournit des recommandations pour un déploiement et une utilisation sécurisés du produit *Zed*. Il vient en complément des guides d'utilisation et documentations techniques [RefPx5], [RefPx6] et [RefPx7] fournis par *Prim'X* afin d'approfondir l'aspect sécurité.

Il s'applique aux SI sur lesquels *Zed* 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 (voir partie 1.4).

Certaines recommandations de ce document peuvent également être transmises aux utilisateurs finaux. La grande diversité des scénarios de déploiement rend cependant le choix des recommandations concernées spécifique à chacun d'entre eux.

Il aborde les problématiques de protection de l'environnement d'exécution du logiciel (partie 3), la gestion des clés de chiffrement (partie 4), les bonnes pratiques d'utilisation du logiciel (partie 5), les politiques de configuration du logiciel (partie 6) ainsi que la protection en intégrité de ces politiques (partie 7).

1.4 Cas d'usage étudié

L'usage retenu dans ce document est un échange sécurisé de fichiers entre plusieurs participants par des moyens informatiques via un réseau non sécurisé, bien que *Zed* puisse répondre à d'autres cas d'usage. La protection locale d'informations n'est ainsi pas abordée, car traitée de manière plus appropriée par *ZoneCentral*, un autre produit de la gamme *Prim'X*.

1.5 Définition des menaces abordées

L'évaluation de la protection que peut apporter *Zed* et, par conséquent, l'émission de recommandations associées à son emploi nécessitent de définir les menaces qui doivent être prises en compte. Le modèle d'attaque défini dans la cible de sécurité de l'évaluation ([RefPx8], paragraphe 3.3) considère un attaquant capable de :

- lire et analyser le fichier conteneur dans lequel est hébergée l'information transmise entre les utilisateurs ;
- obtenir une version du code exécutable du logiciel et l'analyser, l'utiliser tel quel ou en le modifiant ;
- se positionner entre les utilisateurs concernés par l'échange et modifier le fichier conteneur.

Ce document reprend le même modèle d'attaquant.

2

Fonctionnement de Zed

2.1 Présentation des accès sur Zed

Afin de favoriser la compréhension des recommandations qui vont suivre, il est important de préciser le fonctionnement des accès à un conteneur. Ce dernier est un fichier chiffré à l'aide d'une clé dite *clé de conteneur*. Celle-ci est elle-même chiffrée à l'aide de clés d'accès, de différents types énoncés ci-après. Les utilisateurs recourent à une de ces clés d'accès pour déchiffrer la clé de conteneur, et en déchiffrer son contenu.

Zed utilise quatre types de clé d'accès aux conteneurs, chacun d'entre eux correspondant à une clé cryptographique :

- mot de passe ;
- fichier conteneur (PFX, PKCS#12) ;
- carte à puce ou jeton USB (PKCS#11) ;
- conteneur Windows (CSP).

2.2 Limites d'utilisation

Comme mentionné dans le paragraphe précédent, autoriser un utilisateur à lire et écrire dans un conteneur consiste à lui permettre de déchiffrer la clé symétrique de ce conteneur. Or cette clé n'est pas changée durant toute la vie du conteneur. Un utilisateur ayant donc pu la déchiffrer et la mémoriser conserve l'accès au conteneur tout au long de la vie ce dernier.

Il est de plus impossible de changer la clé du conteneur et donc de mettre en place une cryptopériode afin de limiter l'étendue dans le temps d'une éventuelle compromission.

Ces problématiques conduisent à recommander de limiter l'usage des conteneurs à des échanges ponctuels et non à des fins de stockage.

R1

Usage de Zed limité aux échanges et renouvellement des archives

Réserver son usage à des échanges et non à des fins de stockage.
Créer un nouveau conteneur pour chaque échange.

Dans le cas particulier d'un échange entre un utilisateur disposant d'une version gratuite de *Zed* et un utilisateur disposant de la version payante, il est préférable que l'utilisateur disposant de la version gratuite réutilise le conteneur de la version payante pour sa réponse. En effet, cette dernière offre davantage de garanties de sécurité, notamment concernant la taille des clés. Seul l'utilisateur disposant de la version payante créera ainsi les nouveaux conteneurs.

3

Sécurité de l'environnement d'exécution de Zed

Zed 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, confère paragraphe 3.2.2) ;
- du système d'exploitation sur lequel il s'exécute.

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

3.1 Protection physique

R2

Protection physique des postes de travail

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, sinon impossible, de garantir l'intégrité d'un poste informatique si un attaquant a pu avoir un accès à la machine. Il lui est possible de piéger physiquement le matériel ou d'obtenir un accès administrateur sur la machine sans que des mesures défensives logicielles ne puissent apporter de réponse satisfaisante.

3.2 Protection logicielle

3.2.1 Maîtrise du poste utilisateur

R3

Maîtrise des postes de travail

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

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

R4

Homologation Diffusion Restreinte de l'environnement d'exécution

Lorsque les informations protégées sont DR, le poste sur lequel est installé *Zed* et le réseau associé doivent être **homologués pour le traitement d'informations DR**.

Les moyens de filtrage permettant l'isolation du poste utilisateur vis à vis d'Internet doivent être **qualifiés au niveau standard**.

3.2.2 Garantie de l'intégrité du code exécutable

Les fichiers exécutables et les bibliothèques fournies 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 Symantec 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.

R5

Politiques de restriction logicielle de Windows

La mise en œuvre de la protection de l'intégrité des exécutables par les politiques de restriction logicielle Windows dès lors que la mise en œuvre de telles politiques est envisageable dans le SI hôte.

3.2.3 Mise à jour

Il est nécessaire de mettre le produit *Zed* à jour aussi régulièrement que possible. Le dernier build qualifié disponible à la date de rédaction de ce guide est le build 2150. Il permet de corriger les CVE suivantes :

- [CVE-2018-16518]
- [CVE-2019-7312]

4

Gestion des clés d'accès

4.1 Accès par clés asymétriques (accès de type PKCS#12, PKCS#11 ou CSP)

Les clés privées utilisées pour déchiffrer les zones ne doivent pas être accessibles en clair sur le disque de l'utilisateur. En effet, un accès au disque dur du poste de travail suffirait alors à déchiffrer l'ensemble des futurs échanges de l'utilisateur.

R6

Protection des clés privées

La clé privée ne doit jamais être stockée en clair et doit être protégée par un mot de passe.
Le processus de distribution de la clé aux utilisateurs finaux doit intégrer un remplacement du mot de passe de protection dès la réception de celle-ci.

R7

Cryptopériode maximale

La cryptopériode des clés ne doit pas dépasser trois ans.

Il est en effet recommandé de renouveler les clés de manière régulière afin de limiter l'impact d'une compromission de l'une d'entre elles.

R8

Diffusion des clés et des mots de passe

Les bi-clés et les mots de passe associés doivent être diffusés par des canaux distincts.

4.2 Accès par mots de passe

Parmi les différents types d'accès définis dans le paragraphe 2.1, les mots de passe peuvent être distingués des autres. Ils sont dérivés pour former une clé symétrique utilisée pour chiffrer la clé de conteneur.

R9

Protection des mots de passe

Le mot de passe ne doit jamais être stocké en clair (fichier mémo, post-it, etc.).
Le mot de passe doit être transmis aux destinataires via un canal distinct de celui utilisé pour transmettre le conteneur et si possible sécurisé.

Afin d'assurer le respect du besoin d'en connaître et de limiter l'impact d'une éventuelle compromission, il est nécessaire de ne pas réutiliser le même mot de passe pour des conversations différentes.

R10

Unicité et péremption des mots de passe

Utiliser un mot de passe différent pour chaque conversation.
Changer le mot de passe régulièrement, idéalement tous les 3 mois.

La complexité minimale des mots de passe est précisée au paragraphe 6.6.

4.3 Choix des types d'accès

Zed utilise quatre types d'accès aux archives, comme précisé dans la section 2.1.

R11

Choix des types d'accès

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

L'utilisation d'une IGC présente plusieurs avantages. Tous les conteneurs sont accessibles à partir d'un unique secret, au contraire des mots de passe (voir paragraphe 4.2), et les certificats des correspondants peuvent être accessibles au moyen d'un annuaire. De plus, les fonctions de séquestre et de recouvrement permettent aux responsables de la sécurité de déchiffrer une archive en cas d'impératif ou de perte de la clé par un utilisateur. Enfin, un support cryptographique matériel peut assurer la confidentialité et l'intégrité de la clé privée et effectuer les opérations de chiffrement et déchiffrement nécessaires.

R12

Support cryptographique

Privilégier le stockage de la clé cryptographique sur un support cryptographique matériel (carte à puce, token PKCS#11, etc.) autant que possible.

Les bonnes pratiques de configuration de ces types d'accès sont détaillées dans le paragraphe 6.3.

5

Bonnes pratiques d'utilisation

5.1 Liste des accès

Zed n'assure pas la confidentialité de la liste des destinataires. Il n'est pas nécessaire de disposer d'une clé d'accès à une archive pour lire la liste des ces derniers, une instance du logiciel suffit.

R13

Caractère public de la liste des destinataires

Ne pas révéler d'informations sensibles dans la liste des destinataires.

Dans le cas des mots de passe, cette liste contient les *noms d'usage* choisis à leur création.

R14

Caractère public des noms d'usage

Ne pas utiliser le *nom d'usage* comme indication, même partielle du mot de passe.

5.2 Utilisation des clés fonctionnelles

Une clé fonctionnelle est une clé qui n'est pas rattachée à une personne physique mais à une fonction. Elle peut donc être détenue par une ou plusieurs personnes, voire une entité organisationnelle. Elle n'a pas vocation à être changée lors de départs / arrivées d'utilisateurs. Bien qu'il soit préférable d'utiliser une clé personnelle, les besoins opérationnels peuvent nécessiter l'usage de clés fonctionnelles.

Il est recommandé d'utiliser un support physique PKCS#11 de type carte à puce ne permettant pas à son utilisateur d'extraire la clé privée. Ce dernier pourrait sinon conserver la connaissance de cette clé une fois détaché de sa fonction.

R15

Cas des clés fonctionnelles

Dans le cas d'un usage de clés fonctionnelles, il est recommandé de :

- identifier et sensibiliser tous les utilisateurs des clés fonctionnelles ;
- identifier et responsabiliser une unique personne chargée de valider et mettre à jour la liste des utilisateurs des clés fonctionnelles ainsi que de son installation ;
- n'installer la clé fonctionnelle que sur un unique poste sur lequel chaque utilisateur dispose d'un compte nominatif. Chaque accès au poste doit être journalisé et les journaux protégés en intégrité ;

- prévoir une restitution de la clé fonctionnelle par l'utilisateur lors du départ de la fonction ;
- utiliser des supports PKCS#11 ne permettant pas d'extraire la clé privée.

5.3 Intégrité et authenticité des données

Le logiciel *Zed* protège les fichiers stockés dans le conteneur en intégrité, mais certains composants particuliers du conteneur ne sont pas intègres. Si un attaquant supprime ou modifie ces éléments durant la transmission, cela se soldera par une erreur à l'ouverture du conteneur sans relever de problème d'intégrité.

R16

Altération des données déchiffrées

Signaler aux responsables de sécurité tout problème à l'ouverture d'un conteneur.

6

Configuration des politiques

6.1 Modalités de la configuration de Zed

Zed est configurable selon un ensemble de règles qui définissent le comportement du logiciel. Ces règles sont décrites dans le « Manuel des politiques » [RefPx2], lui même résumé dans un « Mémento des politiques » [RefPx1], spécifique à *Zed*.

6.1.1 Environnement AD

Dans un environnement Active Directory, il est possible de configurer le comportement du logiciel *Zed* avec les mécanismes AD.

R17

Configuration par GPO

Dans le cas de postes Windows enregistrés au sein d'un domaine AD, privilégier un déploiement de la configuration de *Zed* via les stratégies de groupe (*GPO*).

Lors de la configuration des stratégies avec l'outil Microsoft *gpedit.msc*, ce dernier ne permet pas d'avoir un aperçu du résultat des stratégies imposées à l'utilisateur final. Il est donc préférable d'utiliser l'outil *Jeu de Stratégies Résultant (RSOP)* ou l'outil *gpresult* afin d'avoir une vision d'ensemble des stratégies réellement appliquées.

La note technique ([AD]) éditée par l'ANSSI détaille les recommandations de sécurité à mettre en place concernant un environnement AD.

6.1.2 Poste Linux

La configuration de *Zed* sur un poste Linux s'effectue à l'aide d'un fichier spécifique. Ce type de déploiement n'est pas couvert par ce document. Les recommandations émises peuvent cependant servir de base non exhaustive pour une configuration de *Zed* sur ce système d'exploitation.

6.2 Contrôle des politiques

Les politiques constituent le cœur de la configuration de *Zed*. Leur bonne application est donc fondamentale pour le bon fonctionnement du logiciel.

Le mode *politiques privées* intervient lorsque l'application des politiques de groupe a échoué et désactive alors l'application de ces dernières. La politique P002 permet d'empêcher un utilisateur malveillant de forcer le passage en mode politique privée.

R18

Mode politiques privées

Désactiver le mode politiques privées en activant la politique P002.

6.3 Restriction des types d'accès autorisés

Les politiques suivantes permettent de limiter les types d'accès autorisés aux utilisateurs :

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

Le choix des types d'accès est précisé dans le paragraphe 4.3. Ce choix est à réaliser selon les cas d'usages envisagés. Il est recommandé de limiter au maximum la surface d'attaque en interdisant l'usage de types d'accès non prévus.

R19

Limitation des types d'accès

Désactiver les types d'accès non prévus dans les scénarios d'utilisation à l'aide des politiques P102 à P105.

6.3.1 Désactivation de l'accès de secours

L'accès de secours est une fonctionnalité de *Zed* qui crée un accès via mot de passe (24 caractères) sur chaque liste d'accès. Ce mot de passe est détenu par l'équipe support. Si l'utilisateur perd sa clé d'accès (oubli de mot de passe, perte de sa carte IGC, etc.), il peut alors appeler l'équipe support pour obtenir le mot de passe de secours et accéder au conteneur. Cependant, le contrôle de l'identité de l'utilisateur par le support n'est pas pris en charge par la solution. Il est donc recommandé de désactiver l'accès de secours.

R20

Désactivation de l'accès de secours

Désactiver la politique P264 afin de d'interdire l'utilisation des accès de secours.



Information

Si l'accès de secours est utilisé malgré tout, il est important de prévoir un processus de vérification d'identité efficace de la personne qui appelle le support.

6.4 Interaction avec l'infrastructure de gestion des clés

Dans le cas d'un utilisateur IGC, (voir paragraphe 1.4), il est possible d'intégrer les outils fournis par l'infrastructure de gestion des clés à l'interface graphique de *Zed* via les stratégies de groupe. Les chapitres suivants présentent ce qui est proposé par le produit.

6.4.1 Accès obligatoires (P131 et P139)

Il est possible d'autoriser des accès qui seront systématiquement ajoutés à l'ensemble des conteneurs. Cela permet notamment de disposer d'un accès administrateur sur l'ensemble des données protégées par *Zed*. Chaque conteneur créé disposera d'un ou plusieurs accès supplémentaires non modifiables.

L'empreinte SHA256 associée à ces accès doit être précisée dans les politiques P139 et P131 afin de s'assurer de leur intégrité. La politique P139 ne concerne que les conteneurs *Zed*, à la différence de la P131, qui s'applique aussi à d'autres produits de chiffrement *Prim'X*.

R21

Séquestre des clés de chiffrement

Dans le cas d'usage d'un utilisateur IGC, privilégier le séquestre des clés plutôt qu'un accès obligatoire aux données protégées.

Bien que la disponibilité des informations protégées au sein des conteneurs soit primordiale, les accès obligatoires sont à éviter. En effet, un seul certificat suffit alors à déchiffrer l'ensemble des informations protégées au sein du SI. Le séquestre des clés permet de récupérer l'accès à des données si l'utilisateur ne peut plus fournir sa clé privée.

6.4.2 Racines autorisées (P141)

Il est possible de limiter les autorités de certification acceptées par *Zed* en renseignant les empreintes SHA256 de leurs certificats dans la politique P141.

R22

IGC autorisées

N'autoriser que les certificats signés par les autorités de certification de l'IGC interne et celles des partenaires en renseignant la politique P141.

6.4.3 Affectation des certificats

R23

Une clé / Un usage

Utiliser des certificats dédiés au chiffrement de clés.

Il est ici question de l'extension « key usage » défini dans la RFC 5280 ([RFC]). Les opérations cryptographiques doivent être réalisées à l'aide de bi-clés différents (signature, chiffrement, etc). Les

contraintes de sécurité qui s'appliquent à ces clés peuvent être incompatibles, il est donc important de disposer d'un bi-clé par usage.

6.4.4 Dates de validité des certificats (P142, P143, P186 et P187)

Il est possible d'autoriser l'utilisation de certificats après leur date de péremption pendant un temps défini. Les politiques P142 et P143 concernent la création de nouveaux accès et les politiques P186 et P187 l'utilisation d'accès déjà existants.

R24

Péremption des certificats

Désactiver la politique P142 pour interdire l'utilisation des certificats périmés lors de la création de nouveaux conteneurs.

Activer la politique P186 afin d'autoriser l'accès à des conteneurs avec un certificat périmé.

Activer la politique P187 pour renseigner une période de grâce autorisant les certificats périmés à accéder aux conteneurs durant une période suffisante (par exemple 365 jours).

Sensibiliser les utilisateurs aux problématiques associées à l'usure des clés.

L'objectif est de respecter la cryptopériode tout en permettant aux utilisateurs de lire des données chiffrées après la date de péremption de leur certificats. *Zed* ne doit cependant pas être utilisé pour du stockage d'information, comme exprimé dans le paragraphe 2.2.

6.4.5 Relaxer le contrôle d'usage (P146)

Par défaut, *Zed* requiert la présence de l'usage « chiffrement de clé » (*KeyUsage=keyEncipherment*) dans les certificats X.509. Il est cependant possible de désactiver cette vérification (et donc d'utiliser des certificats non prévus pour le chiffrement) avec la politique P146.

R25

Contrôle d'usage de clé

Générer et utiliser des certificats disposant de l'usage « chiffrement de clé ».

Conserver le contrôle d'usage de clé de la politique P146 (contrôle strict par défaut).

6.4.6 Utilisation des usages de clé étendus (P148)

Les usages de clé étendus des certificats X.509 ne sont pas utilisés par défaut. Il est cependant possible de configurer *Zed* pour vérifier que la valeur renseignée dans la politique P148 est bien présente dans les usages de clé étendus des certificats. Cette politique peut permettre de s'assurer du respect de la recommandation R23 mais ajoute cependant des contraintes de compatibilité lors de communications avec des correspondants externes. Le choix d'utilisation de la P148 est donc laissé à l'appréciation des responsables.

6.4.7 Annuaire de recherche des certificats de correspondants

Lorsqu'un utilisateur ajoute des accès à un conteneur, il peut rechercher les certificats de ses correspondants dans un ou plusieurs annuaires LDAP. La politique P195 permet de définir ces annuaires selon des modalités définies dans la documentation *Prim'X* [RefPx2].

6.5 Affichage des noms de fichiers et des noms de dossiers au sein d'un conteneur (P233)

Par défaut, *Zed* ne masque pas les noms de fichiers hébergés au sein d'un conteneur. La politique P233 permet de les dissimuler dans les conteneurs créés après l'application de la politique. Cela permet d'éviter la fuite d'informations sensibles par les noms de fichiers.

R26

Caractère public du nom des fichiers chiffrés

Masquer les noms des fichiers contenus au sein des conteneurs (affichés par défaut) en appliquant la P233

Cette politique s'applique uniquement sur les conteneurs créés dans un environnement où la politique est appliquée.

6.6 Contrôle des mots de passe

Il convient de rappeler que l'usage des certificats doit être privilégié, comme exprimé dans la partie 4.3.

6.6.1 Complexité des mots de passe des utilisateurs (P730, P732-742)

Les politiques concernées par la complexité des mots de passe sont les politiques P730 et P732 à P742.

R27

Complexité des mots de passe

Utiliser les valeurs par défaut des politiques P732 à P742.
Passer le seuil d'acceptation de la politique P730 de 80 à 100.

La note technique [MDP] publiée par l'ANSSI et l'article de la CNIL [RefCNIL1] précisent la problématique du choix d'un mot de passe suffisamment complexe.

6.6.2 Authentification unique par Windows (P110)

La politique P110 autorise une authentification unifiée de l'utilisateur (autrement appelée « Single Sign On »). Cependant, cette politique délègue le contrôle de l'accès aux fichiers à Windows et, plus

spécifiquement, au contrôle de session utilisateur. Il suffit alors à un attaquant d'usurper la session de l'utilisateur pour accéder à ses fichiers protégés.

R28

Authentification unifiée

Ne pas activer la politique P110 afin d'interdire l'authentification unique.

6.6.3 Activation du carnet de mots de passe (P750)

Zed propose par défaut aux utilisateurs un registre protégé permettant d'enregistrer leurs mots de passe utilisés pour une utilisation ultérieure. La politique P750 permet de désactiver ce carnet.

R29

Stockage sécurisé des mots de passe

Si le carnet de mots de passe est activé, il ne doit pas contenir de mots de passe de plus de trois mois (comme exprimé dans la recommandation R10).



Information

Le logiciel *KeePass* certifié au premier niveau de sécurité par l'ANSSI peut aussi être utilisé.

6.7 Algorithmes cryptographiques

6.7.1 Algorithme de chiffrement (P290, P291)

La configuration par défaut de *Zed* utilise l'algorithme de chiffrement AES-256. Il est également compatible avec les algorithmes AES-192 ou AES-128 bits. Comme indiqué dans le RGS [RGS], les algorithmes AES-128 et AES-192 sont acceptables, il est cependant préférable, si le SI le permet, d'utiliser la version 256 bits d'AES.

R30

Algorithme de chiffrement

Privilégier l'usage d'AES-256.

6.7.2 Algorithme de hachage (P292)

La politique P292 configure l'algorithme de hachage utilisé par le produit. Cet algorithme intervient notamment durant la dérivation de clés à partir de mots de passe.

R31

Algorithme de hachage

Ne pas modifier les valeurs par défaut de la politique P292 afin de préférer SHA256 à SHA1.

L'algorithme SHA1 n'est pas recommandé car il n'est plus considéré comme conforme à l'état de l'art ([RGS]).

6.7.3 Dérivation des mots de passe (P290, P291, P293, P294 et P295)

Un accès de type mot de passe se fait à l'aide d'une clé de chiffrement dérivée d'un mot de passe renseigné par l'utilisateur.

Les paramètres de dérivation sont les suivants :

- l'algorithme utilisé (P292, SHA-256 par défaut) ;
- la taille du sel (P293, 8 octets par défaut) ;
- le nombre de tours lors de la dérivation (P294, 100 000 par défaut) ;
- la taille du vecteur de vérification, une chaîne utilisée pour vérifier la validité du mot de passe de l'utilisateur lors de l'accès à un conteneur (P295, 8 octets par défaut).

Les valeurs par défaut sont satisfaisantes.

R32

Dérivation de clés

Ne pas modifier les valeurs par défaut des politiques P290, P291, P293, P294 et P295 afin de ne pas affaiblir la dérivation des clés.

6.7.4 Cartes et jetons PKCS#11 supportés et autorisés (P296)

Par défaut, *Zed* est compatible avec un nombre limité de cartes et jetons PKCS#11. Cette politique permet d'indiquer les emplacements de bibliothèques PKCS#11 de fournisseurs non supportés par défaut afin de pouvoir les utiliser avec *Zed*. Dans le cas où cette politique est activée, le produit utilise uniquement les fournisseurs renseignés.

R33

Support matériel spécifique

Renseigner les bibliothèques PKCS#11 utilisées dans la politique P296 afin de limiter l'usage des cartes et jetons à ceux autorisés.

6.7.5 Conteneurs v2 (P399)

La structure des conteneurs a été modifiée afin de sécuriser au mieux les résidus de fichier. Il y a cependant une rupture de compatibilité avec les versions précédentes des conteneurs.

R34

Conteneurs v2

Utiliser les conteneurs v2 en activant la politique P399 et vérifier la compatibilité du chiffrement avec les correspondants.

6.7.6 PKCS#1 v2.2 (P383)

Il est désormais possible d'utiliser OAEP plutôt que la version 1.5 de PKCS#1 qui corrige un certain nombre de vulnérabilités, notamment face à des attaques à clair choisi.

R35

PKCS#1 v2.2

Utiliser la version 2.2 de PKCS#1 en activant la politique P383.

6.8 Correction de la CVE-2018-16518

L'image de marque, *watermark* en anglais, permet au logiciel *Zed* d'afficher un fond personnalisé lors de l'ouverture du conteneur. C'est un outil purement esthétique. Dans le build 2120, l'image de marque n'est pas intègre et représente un vecteur d'attaque potentiel pour un attaquant. Cette vulnérabilité a été reportée dans la CVE-2018-16518 et est corrigée dans le build 2121. Il est donc fortement recommandé de mettre à jour le logiciel *Zed*.

R36

Désactivation de l'image de marque

Vérifier le build actuel de *Zed* et, si nécessaire, le mettre à jour vers le build 2150.



Attention

Il est possible d'utiliser la politique P289 avec le mot clé "DisableWatermark" à 1 pour désactiver l'utilisation du Watermark. Cependant cette mesure ne doit pas être considérée comme un correctif de la vulnérabilité à long terme mais temporaire, le temps de migrer vers le build qui corrige la vulnérabilité.



Information

Même une fois *Zed* à jour, le Watermark n'étant que purement esthétique, il est possible de le désactiver si il n'est pas utilisé.

7

Signature des politiques

Par défaut, le produit *Zed* accepte toutes les stratégies de groupes fournies par l'AD. Il est cependant possible de configurer le logiciel pour accepter uniquement des jeux de politiques signés afin de contrer une attaque diffusant un ensemble de politiques malveillant.

R37

Signature des politiques

Signer les GPO selon le guide [RefPx3] fournit par *Prim'X* .

Liste des recommandations

R1	Usage de <i>Zed</i> limité aux échanges et renouvellement des archives	8
R2	Protection physique des postes de travail	9
R3	Maîtrise des postes de travail	10
R4	Homologation Diffusion Restreinte de l'environnement d'exécution	10
R5	Politiques de restriction logicielle de Windows	10
R6	Protection des clés privées	11
R7	Cryptopériode maximale	11
R8	Diffusion des clés et des mots de passe	11
R9	Protection des mots de passe	12
R10	Unicité et péremption des mots de passe	12
R11	Choix des types d'accès	12
R12	Support cryptographique	12
R13	Caractère public de la liste des destinataires	13
R14	Caractère public des noms d'usage	13
R15	Cas des clés fonctionnelles	14
R16	Altération des données déchiffrées	14
R17	Configuration par GPO	15
R18	Mode politiques privées	16
R19	Limitation des types d'accès	16
R20	Désactivation de l'accès de secours	16
R21	Séquestre des clés de chiffrement	17
R22	IGC autorisées	17
R23	Une clé / Un usage	17
R24	Péremption des certificats	18
R25	Contrôle d'usage de clé	18
R26	Caractère public du nom des fichiers chiffrés	19
R27	Complexité des mots de passe	19
R28	Authentification unifiée	20
R29	Stockage sécurisé des mots de passe	20
R30	Algorithme de chiffrement	20
R31	Algorithme de hachage	20
R32	Dérivation de clés	21
R33	Support matériel spécifique	21
R34	Conteneurs v2	21
R35	PKCS#1 v2.2	22
R36	Désactivation de l'image de marque	22
R37	Signature des politiques	23

Bibliographie

- [RFC] *RFC 5280*.
Page web, Network Working Group, mai 2008.
<https://tools.ietf.org/html/rfc5280>.
- [RefPx6] *Zed Limited Edition 6.1 Guide*.
Externe PX156523r1, PRIMX, octobre 2015.
- [RefPx7] *Cible de sécurité Zed 6.1*.
Externe, PRIMX, 2016.
https://www.ssi.gouv.fr/uploads/2016/05/anssi_cible2016_25en.pdf.
- [RefAn2] *Rapport de certification Zed 6.1 b2120*.
Interne, ANSSI, 2016.
https://www.ssi.gouv.fr/uploads/2016/05/anssi-cc-2016_25fr.pdf.
- [RefPx3] *Mise en oeuvre de la signature des politiques*.
Externe PX13C133, PRIMX, juillet 2017.
- [RefPx1] *Mémento des politiques*.
Externe PX156520r5, PRIMX, juillet 2017.
- [RefCNIL1] *Authentification par mot de passe : les mesures de sécurité élémentaires*.
Page web, CNIL, novembre 2018.
<https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>.
- [CVE-2018-16518] *CVE-2018-16518*.
Page web, MITRE, septembre 2018.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16518>.
- [RefPx5] *Guide d'utilisation des conteneurs chiffrés*.
Externe PX156518r65, PRIMX, octobre 2018.
- [RefPx2] *Manuel des politiques*.
Externe PX156524r25, PRIMX, novembre 2018.
- [CVE-2019-7312] *CVE-2019-7312*.
Page web, MITRE, janvier 2019.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7312>.
- [RefPx8] *Fix Notes*.
Externe PX161537r2242, PRIMX, janvier 2019.
- [RefAn1] *Qualification au niveau standard Zed 6.1 b2150*.
Interne, ANSSI, 2019.
https://www.ssi.gouv.fr/uploads/2019_574_np.pdf.
- [MDP] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
<https://www.ssi.gouv.fr/mots-de-passe>.

- [AD] *Recommandations de sécurité relatives à Active Directory.*
Note technique DAT-NT-017/ANSSI/SDE/NP v1.1, ANSSI, septembre 2014.
<https://www.ssi.gouv.fr/Active-Directory>.
- [RGS] *Référentiel général de sécurité (RGS).*
Référentiel Version 2.0, ANSSI, juin 2012.
<https://www.ssi.gouv.fr/rgs>.
- [ETALAB] *Licence ouverte / Open Licence.*
Page Web v2.0, Mission Etalab, avril 2017.
<https://www.etalab.gouv.fr/licence-ouverte-open-licence>.

ANSSI-PG-068
Version 1.1 - 14/11/2019
Licence ouverte / Open Licence (Étalab - v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

