Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

DGNUM

Paris, le 15 mai 2019

N°170/ARM/DGNUM/DG/NP

DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

Le directeur général

NOTE

à l'attention des

destinataires *in fine*

OBJET : outil de chiffrement de fichiers *Zed!* pour les échanges externes au ministère et hors industriels d'armement.

PIÈCE JOINTE : annexe I – concept d'emploi de *Zed!*.

Conformément aux conclusions du dernier Sous-comité 3 du CODIR des Intranets, la DGNUM diffuse le concept d'emploi du logiciel de chiffrement de fichiers *Zed!*.

ACID reste par ailleurs le seul outil autorisé de chiffrement et de signature de documents au sein du ministère et dans le cadre d'échanges avec les industriels de l'armement.

Zed! pourra donc être mis à disposition des agents du ministère après justification du besoin, pour les échanges avec des personnes morales ou physiques externes au ministère des Armées, hors industriels de l'armement qui doivent utiliser *ACID*.

La DGNUM demande à la DIRISI de bien vouloir mettre à disposition le logiciel pour la fin de mai 2019.

Le vice-amiral d'escadre Arnaud COUSTILLIÈRE
directeur général du numérique et des systèmes
d'information et de communication,



60 boulevard du général Martial Valin – CS 21623 – 75509 PARIS CEDEX 15
Tél : 09.88.67.91.74 – PNIA : 841.167.93.74
florian.crosnier@intradef.gouv.fr

DESTINATAIRES :

- EMA ;
- SGA ;
- DGA ;
- DGSE ;
- DRSD ;
- DC DIRISI.

COPIES :

- Cab MinArm ;
- DPID/FSSI ;
- Archives.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

Concept d'emploi de Zed!

1ère édition

approuvée le 14 mai 2019

Document entretenu par la DGNUM



L'édition en vigueur de ce document est celle accessible via le site DGNUM.
S'assurer de la validité de toute copie avant usage.

Sommaire

1 INTRODUCTION 5
2 CADRE GENERAL D'EMPLOI 5
2.1 ACID 5
2.2 ZED! 6
2.3 COMPLEMENTARITE D'ACID ET DE ZED! 6
3 CONCEPT D'EMPLOI DE ZED! A DESTINATION DES USAGERS 6
3.1 ÉCHANGES AVEC UN ORGANISME EXTERNE OU UNE SOCIETE PRIVEE 6
3.2 PROTECTION DES IDENTITES 7
3.3 PROTECTION DES SECRETS 7
4 CONCEPT D'EMPLOI A DESTINATION DES ADMINISTRATEURS 8
4.1 JUSTIFICATION PREALABLE AU DEPLOIEMENT 8
4.2 FILTRAGE DES ARCHIVES NON CONFORMES 8
4.3 MASQUAGE DES NOMS DES FICHIERS 8
4.4 ACCES AUX ARCHIVES 8
5 REFERENCES 9

1 INTRODUCTION

Le rapport annuel 2018 de l'ANSSI présente l'espionnage comme le principal risque visant les organisations. Réalisé par des individus, des organisations ou des États, le cyber-espionnage peut prendre plusieurs formes et émaner d'une multitude de sources. Le ministère des armées, en relation directe avec les industriels de l'armement, est une cible avérée pour les organisations étatiques.

Pour se prémunir contre cette menace, il convient de sensibiliser les personnels du ministère au risque cyber, et de les inciter à chiffrer[1] leurs documents et courriers électroniques sensibles[2].

Ce document a pour but de décrire le cadre d'emploi du système de chiffrement de fichiers *Zed!* pour des échanges de fichiers dans des cas où l'usage d'*ACID* n'est pas requis. [CE_ACID]

Il donne également un aperçu des cadres de pilotage et de l'organisation du soutien qui accompagnent la mise en œuvre du service. Cette dernière doit être complétée par la DIRISI par des documents plus détaillés en tant que de besoin.

2 CADRE GENERAL D'EMPLOI

Le chiffrement de fichiers avec un logiciel qualifié par l'ANSSI doit être utilisé pour tous les échanges sensibles sur des réseaux non protégés (Internet…). [II_901]

Le chiffrement de fichiers stockés sur un support externe ou amovible (exemple : clé USB) ou sur un moyen nomade (exemple : PC portable) permet d'éviter de le traiter comme un support ou un terminal sensible ou diffusion restreinte et de réduire le risque lié à sa perte ou à son vol.

2.1 ACID

Le ministère des Armées procède au chiffrement des fichiers ou des courriers électroniques de niveau sensible ou diffusion restreinte (éventuellement avec une mention spéciale comme Spécial France ou Confidentiel Personnel) ou retreint OTAN ou restreint UE à l'aide de l'outil *ACID Cryptofiler*. Cette solution a pour avantages d'être maîtrisée par le ministère, d'offrir un niveau de chiffrement élevé, et de reposer exclusivement sur des certificats électroniques[3].

Cependant, *ACID Cryptofiler* ne peut être distribué hors du ministère des Armées ou industriels ayant un contrat d'armement avec le ministère sans accord de l'EMA voire du SGDSN ; de plus, son utilisation nécessite au préalable l'authentification et la remise d'une bi-clé à chaque utilisateur. Les clients d'*ACID* sont principalement les personnels du ministère des Armées, certains organismes de défense[4], et les industriels travaillant au profit du ministère des Armées. Cette solution n'est donc pas adaptée au chiffrement d'échanges avec des organismes interministériels, d'autres ministères ou certaines sociétés privées.

La disponibilité de *Zed!* pour les agents du ministère permet uniquement de combler un périmètre que le logiciel *ACID* ne peut pas couvrir. L'existence *d'ACID* au sein du ministère des Armées n'est pas remise en question. Son maintien en conditions opérationnelles et de sécurité est assuré, et son interface utilisateur est vouée à évoluer pour gagner en ergonomie (notamment par l'intégration d'un plug-in de messagerie dès la mise en place de Windows 10).

---

[1] Rendre une information illisible par quiconque ne possède pas la clé de déchiffrement associée.

[2] Au sens Diffusion Restreinte, voire Spécial France, mais aussi au sens couvert par le secret professionnel ou par un domaine de confidentialité règlementaire : personnel, médical, commercial, diplomatique, etc.

[3] Les certificats sont au format « *ACID* » qui est un format spécifique. Néanmoins, les versions ultérieures pourraient utiliser un format standard de certificat électronique.

[4] Avec la généralisation du logiciel *Zed!* en interministériel, la liste des organismes externes au ministère des Armées disposant d'*ACID* diminuera progressivement jusqu'à éventuellement disparaitre.

2.2 Zed!

Le logiciel *Zed!* édité par la société française Prim'X permet également de chiffrer des fichiers. Les archives *.zed* peuvent être créées via l'utilisation de mots de passe ou de certificats électroniques standards (l'usage de certificats n'étant pas prévu au ministère des Armées à ce jour, cet aspect n'est pas abordé dans ce concept d'emploi ; il pourra faire l'objet d'une mise à jour éventuelle).

- ***Zed!*** dans sa version disponible pour les administrations de l'État français (licence globale pour les besoins interministériels), et ***Zed! Entreprise*** (licence payante) fournissent toutes les fonctionnalités de chiffrement, déchiffrement et signature de fichiers et conteneurs. **Ce sont les seules versions qualifiées par l'ANSSI, qui doivent donc être utilisées pour la protection des informations de niveau sensible, diffusion restreinte (éventuellement avec une mention spéciale), restreint UE ou restreint OTAN ;**
- ***Zed! Free*** est le pendant gratuit du logiciel. Il permet de consulter des archives *.zed* et potentiellement de chiffrer, mais avec un niveau de robustesse insuffisant pour des informations sensibles. Le chiffrement de fichiers avec *Zed! Free* n'est donc pas autorisé. Les archives créées à partir de *Zed! Free* peuvent faire l'objet d'un filtrage sur les passerelles du ministère.

Les fichiers ainsi chiffrés et archivés au format *.zed* peuvent être communiqués à travers un canal non protégé tel qu'Internet ou via des supports non protégés (ex : clé USB).

2.3 Complémentarité d'ACID et de Zed!

Le logiciel *ACID*, contrairement à *Zed!*, ne permet pas l'usage de mots de passe partagés. De ce fait, l'usage d'*ACID* n'est pas vulnérable aux mauvaises pratiques concernant la gestion des mots de passe (notamment les modalités de transmission du mot de passe vers les destinataires de l'archive *Zed!* ou la réutilisation d'un même mot de passe sur plusieurs communautés de besoin d'en connaitre).

De ce fait :

- le logiciel *ACID* est le seul logiciel devant être utilisé au sein du ministère des armées ou dans le cadre d'échanges avec les industriels ayant un contrat d'armement avec le ministère des Armées ;
- le logiciel *Zed!* doit être utilisé dans le cadre d'échanges avec des personnes physiques ou morales publiques ou privées hors du ministère[5], ou avec les industriels n'ayant pas de contrat d'armement avec le ministère des Armées ;
- la seule version de *Zed!* utilisable par les agents du ministère est celle validée par l'ANSSI et disponible uniquement auprès de la DIRISI.

3 CONCEPT D'EMPLOI DE ZED! A DESTINATION DES USAGERS

3.1 Échanges avec un organisme externe ou une société privée

Tout fichier portant des informations non classifiées de sensibilité supérieure à « non protégé » et qui est destiné à circuler sur Internet à destination de personnes morales ou physiques externes au ministère des Armées, hors industriels de l'armement, ne disposant pas d'*ACID*, doit être chiffré avec *Zed!*.

Zed! Free permet de déchiffrer des archives *.zed*. Il est gratuit pour un usage professionnel et disponible sur Windows, Linux, Mac OS, Android et iOS.

R-1	*Zed! Free* ne doit pas être utilisé par le ministère des Armées, il s'agit d'une facilité pour les destinataires qui ne pourront alors pas transmettre en retour de document sensible ou Diffusion Restreinte.

[5] Exemple : échange dans le cadre d'un groupe de travail relatif à l'aviation civile auquel le ministère des Armées participe et intégrant des opérateurs privés. Dans ce cadre, les échanges avec Airbus peuvent être réalisés via l'usage de *Zed!*.

3.2 Protection des identités

Zed! ne permet pas de masquer la liste des destinataires d'une archive. Toute personne mettant la main sur une archive *.zed* peut lire les informations d'identité des destinataires.

La liste des destinataires peut dans certains cas être une information sensible : le risque de subversion induit sur ces destinataires doit être mesuré par l'émetteur de l'archive.

R-2	L'identité des destinataires ne doit pas comprendre d'informations sensibles.

Notamment, les identifiants choisis pour accéder aux archives ne doivent pas permettre d'associer l'identité d'une personne avec son éventuel statut de militaire (armée d'appartenance, grade…)[6].

3.3 Protection des secrets

Compte tenu de la difficulté liée à la gestion de mots de passe partagés, les archives *.zed* sont surtout destinées à faire transiter des informations sensibles sur des réseaux non protégés. Elles doivent donc être considérées comme éphémères et ne doivent pas être utilisées pour l'archivage des fichiers. Les fichiers peuvent être stockés en clair sur des répertoires partagés Intradef ou sur des postes terminaux homologués au bon niveau[7]. *ACID* peut également être utilisé pour l'archivage de fichiers, notamment dans le cas de mentions spéciales comme Confidentiel Personnel ou Spécial France.

La gestion des mots de passe peut être simplifiée par l'utilisation du carnet de mots de passe de *Zed!*. Cet outil permet de stocker de façon sécurisée les mots de passe définis pour les différentes archives envoyées ou reçues sur un compte utilisateur. Il permet également de générer des mots de passe aléatoires respectant la politique de configuration du logiciel. C'est la solution à privilégier pour définir les mots de passe des archives.

R-3	Les mots de passe d'archives doivent respecter les critères de robustesse suivants : - être composés d'au moins 10 caractères uniques ; - comprendre au moins deux lettres minuscules uniques ; - comprendre au moins deux lettres majuscules uniques ; - comprendre au moins un symbole (ponctuation, parenthèse, astérisque…) ; - comprendre au moins un chiffre.

R-4	La clé privée ou le mot de passe de déchiffrement d'une archive ne doit pas être stocké sur le même support que l'archive.

R-5	Pour les transferts, l'archive et son mot de passe ne doivent pas être envoyés par le même canal de transmission : - Exemple d'échange valide : envoi de l'archive par mail et envoi du mot de passe par SMS ; - Exemple d'échange non valide : envoi de l'archive par mail et envoi du mot de passe dans un second mail.

R-6	Les mots de passe des archives *.zed* ne doivent jamais être stockés en clair et ne doivent pas être réutilisés (exception tolérée pour la réutilisation : archives échangées dans le cadre d'une même communauté dans laquelle il n'y a pas nécessité de gérer le besoin d'en connaître).

[6] Conformément à l'article 117 de la loi n°2016-731 du 3 juin 2016.

[7] Il est fait l'hypothèse qu'un PC homologué Diffusion Restreinte bénéficie d'un chiffrement de surface de niveau Diffusion Restreinte. Dans le cas contraire un chiffrement *ACID* est nécessaire pour le stockage de document Diffusion Restreinte.

4 CONCEPT D'EMPLOI A DESTINATION DES ADMINISTRATEURS

4.1 Justification préalable au déploiement

R-7	Afin de restreindre l'usage de *Zed!* aux seuls scénarii prévus, le logiciel ne doit être déployé que pour les utilisateurs en exprimant le besoin par une demande spécifique.

Les demandes d'installation doivent se faire par un ticket APSI-GI accompagné d'une justification validée par l'OSSI ou le correspondant SSI de l'entité du demandeur.

4.2 Filtrage des archives non conformes

R-8	Tout fichier non conforme au format d'archive *.zed* et/ou issu d'une version de *Zed!* non qualifiée par l'ANSSI devra être rejeté, et les émetteurs ou destinataires de l'archive identifiés au sein du ministère devront en être notifiés.

Toutes les versions de *Zed!* ne sont pas qualifiées par l'ANSSI, le logiciel permet de créer des archives non conformes à la décision de qualification. Ceci est notamment systématiquement le cas pour les archives créées avec le logiciel *Zed! Free*.

Les passerelles permettant le transfert d'archive *Zed!* entre un espace « Diffusion Restreinte »[8] (ou équivalent) et un espace « non protégé »[9] doivent, dans la mesure du possible, vérifier que l'archive est conforme à la décision de qualification de l'ANSSI[10].

4.3 Masquage des noms des fichiers

R-9	Les noms de fichiers contenus dans les archives *.zed* ne doivent pas être lisibles par une personne ne possédant pas le mot de passe ou la clé de déchiffrement.

Par défaut, les noms des fichiers contenus dans une archive *.zed* sont lisibles même pour une personne ne possédant par la clé de déchiffrement. Les noms des fichiers peuvent permettre à un tiers malveillant de déduire des informations sensibles.

Cette fonction existe dans les politiques de configuration du logiciel.

4.4 Accès aux archives

R-10	Aucun mécanisme d'accès à l'ensemble des archives générées par les utilisateurs du ministère des Armées ne doit être activé.

Zed! offre la possibilité, par le biais de stratégies de groupe, de forcer l'ajout d'un accès aux archives créées par tous les utilisateurs. Cette fonction permet, même en cas de perte du mot de passe d'une archive, de la déchiffrer grâce à cet accès supplémentaire.

Cette fonction introduit le risque critique de pouvoir déchiffrer l'ensemble des archives produites par le ministère des Armées en volant ou reproduisant cette clé.

[8] Exemple : INTRADEF

[9] Exemple : Internet

[10] Notamment sur la robustesse de l'algorithme de chiffrement utilisé et sur les métadonnées contenues dans les archives.

5 REFERENCES

[RGS]	Référentiel Général de Sécurité version 2.0 du 13 juin 2014
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles n°901/SGDSN/ANSSI du 11 février 2015
[AGR_ZED]	Agrément *Zed!* de référence 574/ANSSI/SDE/PSS/BQA du 11 février 2019
[CE_ACID]	Concept d'emploi d'*ACID Cryptofiler V7* diffusé par note n°D-10-000598/DEF/EMA/CPI/SSI/DR du 6 août 2010