RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# ZED-FILES : Aux frontières du réel

# Sommaire

# 1. INTÉRÊT DE LA CIBLE

# La mention « Diffusion Restreinte »

**DIFFUSION RESTREINTE**

Ce document ne doit être communiqué qu'aux personnes qualifiées pour le connaitre.

- Protection d'information « sensible »
- Classification, Pénal
- Régie par l'II 901*

Transport et stockage

[…] chiffrées à l'aide de **moyens agréés** [pour le niveau DR] par l'ANSSI

VISA DE SÉCURITÉ

*Instruction Interministérielle

# Visa de sécurité

## Modèles

### Certification :

- Cible de sécurité
- Evaluation CC / CSPN
- Choix du CESTI / Paiement
  - Par le client
  - Mais dans une liste de prestataires reconnues par l'ANSSI

### Qualification :

- Objectif de recommandation
- Cible avec fonctions de sécurité pour un niveau d'attaquant
  - Élémentaire
  - Standard
  - Renforcé
- Visée règlementaire
- Engagements du fournisseur

### Agrément :

- Permet l'utilisation d'une solution dans certains cadres règlementaires

https://cyber.gouv.fr/visa-de-securite

# Visa de sécurité

## Cible et garanties


Garantie de sécurité **absolue**

- *« Des moyens ont été mis en œuvre pour en jauger le niveau de sécurité, lié à un niveau d'attaquant »*

- Pour une cible donnée
  - Ex: EDR avec un VISA ➔ robuste contre des LPE, ne dit rien sur sa capacité à détecter ou bloquer
  - Ex: Passerelle dont la cible ne contient pas l'interface d'administration Web ➔ présence possible de vulnérabilités Web, même triviales
  - Ex: Visioconf' avec un VISA sans agrément DR ➔ ne permet pas de faire de la visioconf' DR au travers d'Internet, mais comme tout autre logiciel de visioconf' peut être utilisé au sein d'un réseau DR

# Agrément Zed!

## Le parcours du RSSI étudiant

### 0. *Listing* des produits agréés

# Agrément Zed!

## Le parcours du RSSI étudiant

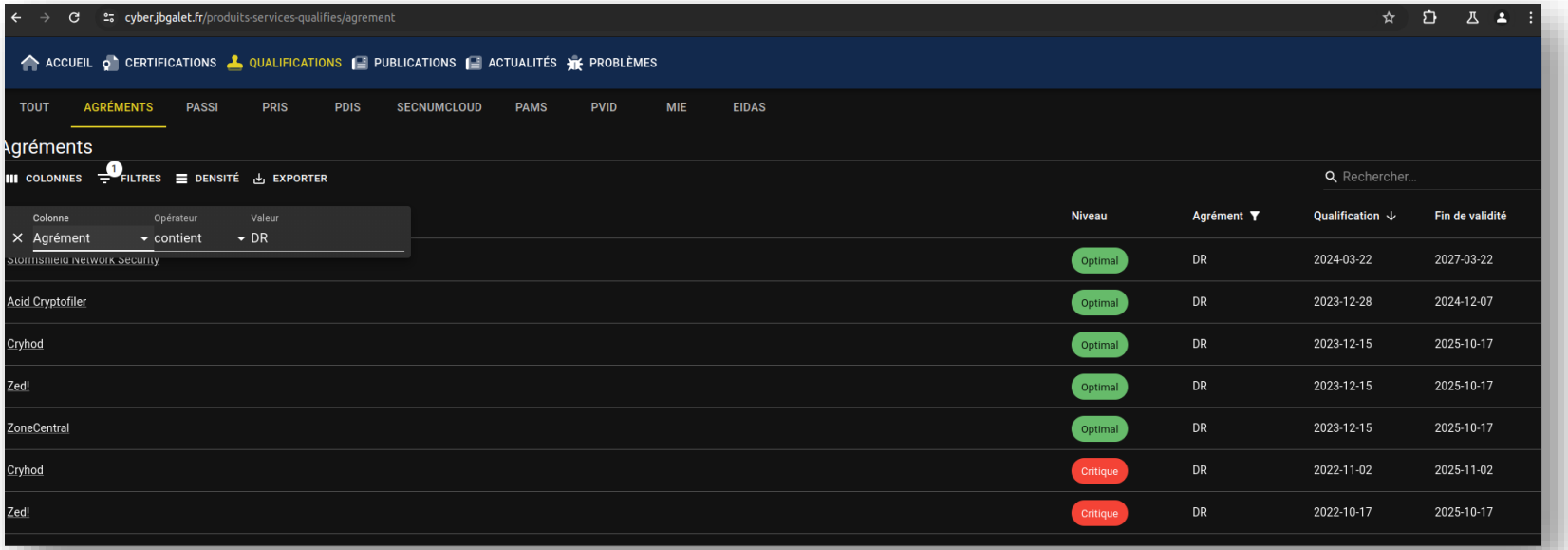
0. *Listing* des produits agréés

# Agrément Zed!

## Le parcours du RSSI pressé

https://cyber.jbgalet.fr/produits-services-qualifies

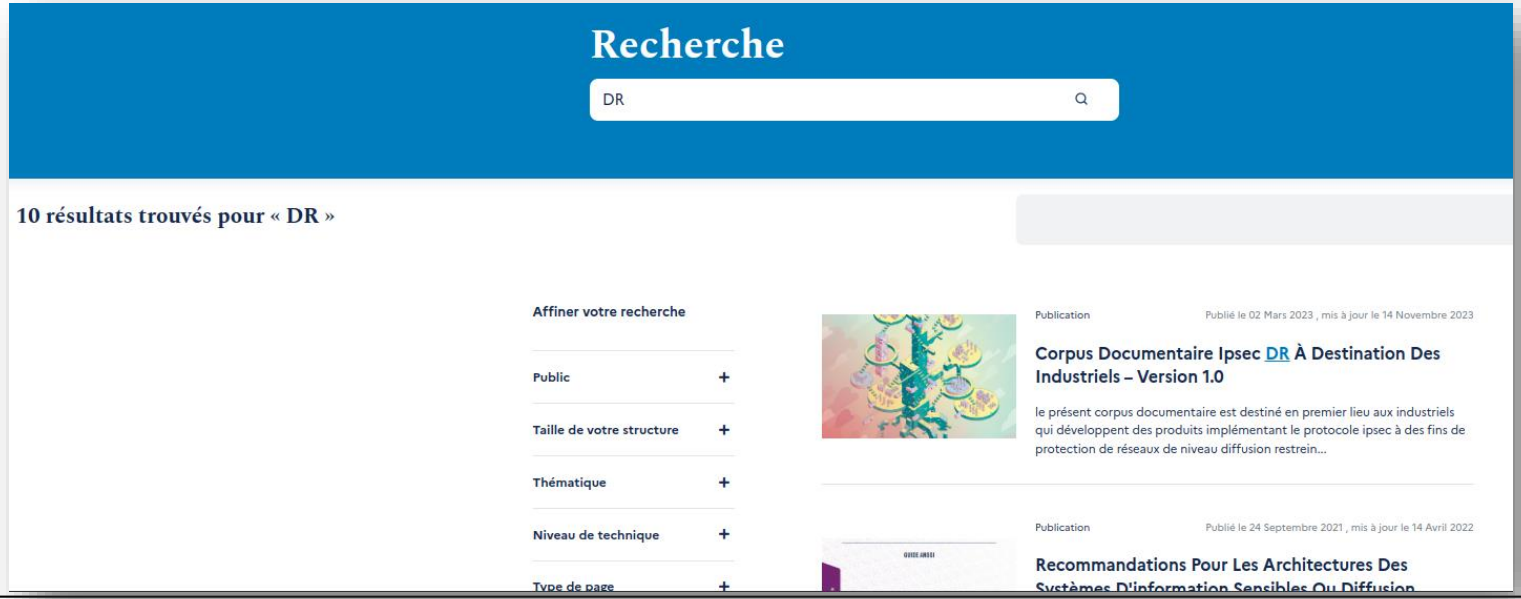
0. *Listing* des produits agréés



# Agrément Zed!

## Le parcours du RSSI persévérant

0. *Listing* des produits agréés



# Agrément Zed!

## Le parcours du RSSI persévérant

0. *Listing* des produits agréé

Produit/service qualifié — Publié le 03 Juin 2024 , mis à jour le 03 Juin 202

**Zed!**

Produit/service qualifié — Publié le 03 Juin 2024 , mis à jour le 03 Juin 202

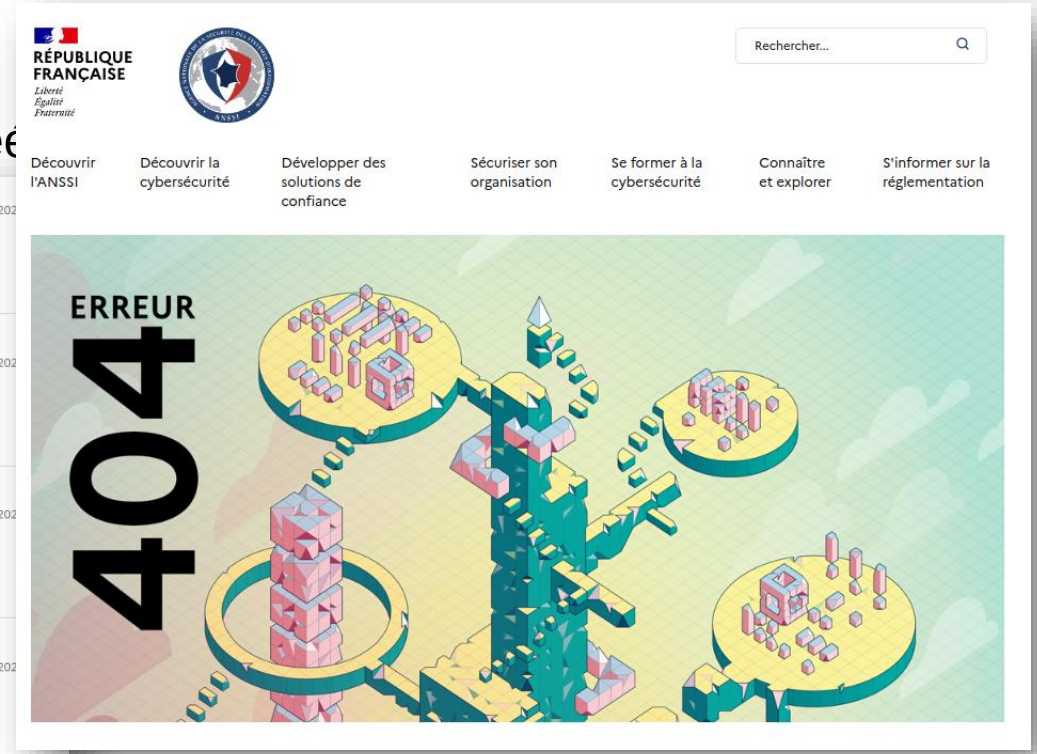
**Cryhod**

Produit/service qualifié — Publié le 03 Juin 2024 , mis à jour le 03 Juin 202

**Stormshield Network Security**

Produit/service qualifié — Publié le 03 Juin 2024 , mis à jour le 03 Juin 202

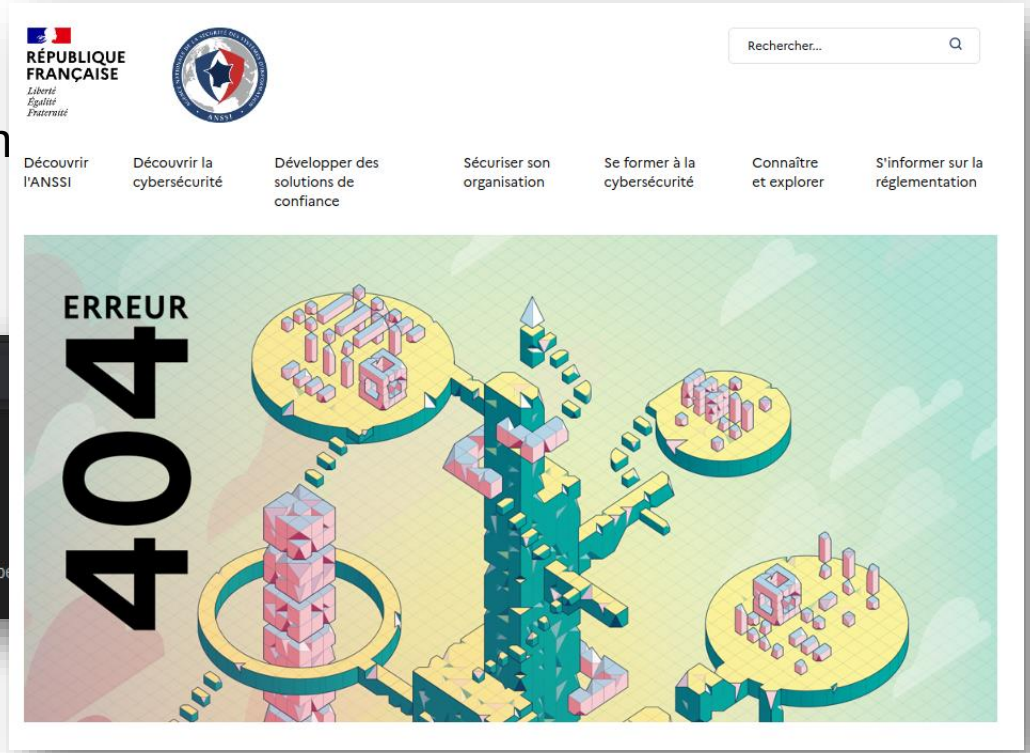
**Zed!**



# Agrément Zed!

## Le parcours du RSSI connaisseur

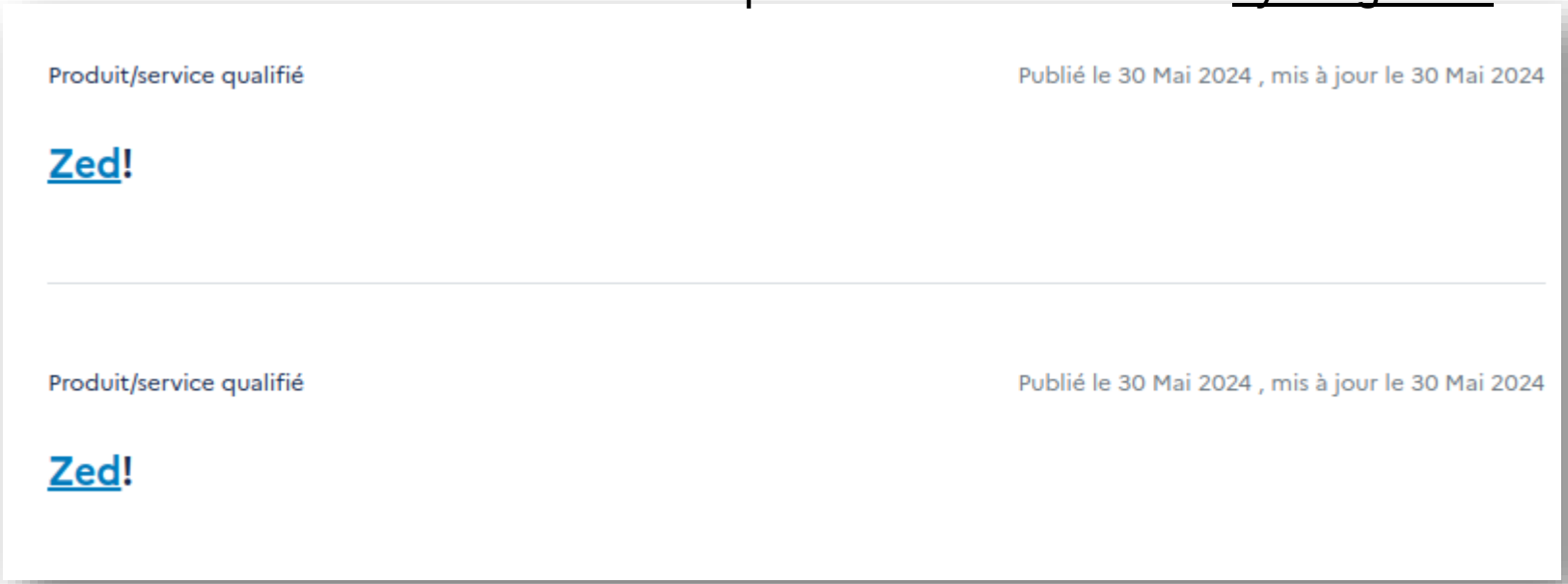
1. Recherche de la décision

# Agrément Zed!

## Le parcours du RSSI avisé et chanceux

1. Recherche de la décision de qualification de Zed! sur cyber.gouv.fr



Produit/service qualifié

Publié le 30 Mai 2024 , mis à jour le 30 Mai 2024

Zed!

Produit/service qualifié

Publié le 30 Mai 2024 , mis à jour le 30 Mai 2024

Zed!

# Agrément Zed!

## Le parcours du RSSI avisé et (mal)chanceux

### 2. (Pour chaque?) Consultation de la décision

| | |
|---|---|
| Nom du fournisseur | Prim X Technologies |
| Date de début de qualification | 17/10/2022 |
| Date de fin de qualification | 17/10/2025 |
| Référence de la décision de qualification | 1 |
| Version | Q.2021.1 |
| Niveau d'agrément | DR |
| Niveau de recommandation | ✔ - Optimal |

**Décision de qualification**

PDF 2022_2241_np.pdf

| | |
|---|---|
| Nom du fournisseur | Prim X |
| Date de début de qualification | 15/12/2023 |
| Date de fin de qualification | 17/10/2025 |
| Référence de la décision de qualification | 3 |
| Version | Q2021.X avec X>=2 |
| Niveau d'agrément | DR |
| Niveau de recommandation | ✔ - Optimal |

**Décision de qualification**

PDF 2023_2173_np.pdf

# Agrément Zed!

## Le parcours du RSSI avisé

3. *Double-check* sur le site de l'éditeur

### DETAILS

+ CVEID: 2023-50444 (created on 12/10/2023)

### AFFECTED PRODUCTS AND VERSIONS

+ ZED! Enterprise for Windows version prior to 2023.5, including versions Q.2020.1, Q.2020.2 and Q.2021.1
+ ZED! features in ZONECENTRAL for Windows version prior to 2023.5, including versions Q.2021.1
+ ZED! features in ZEDMAIL for Windows version prior to 2023.5

### SOLUTIONS AND RECOMMENDATIONS

Depending on your solution, upgrade to one of the following versions:

+ ZED! Enterprise for Windows version ~~Q.2020.5 (version validated by ANSSI)~~
+ ZED! Enterprise for Windows version Q.2021.2 (version validated by ANSSI)
+ ZED! Enterprise for Windows minimal version 2023.5
+ ZED! features in ZONECENTRAL for Windows version Q.2021.2 (version validated by ANSSI)
+ ZED! features in ZONECENTRAL for Windows minimal version 2023.5
+ ZED! features in ZEDMAIL for Windows minimal version 2023.5

For more information, contact support[@]primx[.]eu.

# Agrément Zed!

## Le parcours du RSSI avisé

4. Lecture de (la bonne) décision de qualification

Décide :

Art. 1er – Le produit fourni par la société PRIM'X TECHNOLOGIES portant le nom « ZED ! » en version Q2021.X avec X≥2 respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 et est qualifié au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 2 – Le produit fourni par la société PRIM'X portant le nom « ZED ! » en version Q2021.X avec X≥2 est agréé pour la protection d'informations marquées Diffusion Restreinte ou classifiées Diffusion Restreinte OTAN/NATO Restricted ou Restreint UE/UE Restricted sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 3 – La présente décision est valable jusqu'au 17 octobre 2025.

Vincent STRUBEL
Directeur général de l'agence nationale de la sécurité des systèmes d'information

**Annexe**

Conditions et limites de la qualification.

Références

| | |
|---|---|
| [1]. | Rapport de certification, ANSSI-CC-2022/40, 23/08/2022. |
| [GUIDE_INSTALL]. | Zed! Q.2021.1 Guide d'installation FR, référence PX20A1391, version 1.0 ; |
| [GUIDE_ADMIN]. | Manuel des politiques Zed ! Q.2021 FR, référence PX20A1376r3 ; |
| [GUIDE_UTIL]. | Zed! Q.2021 Guide d'utilisation des conteneurs chiffrés FR, référence PX20A1397r3 |

**Conditions**

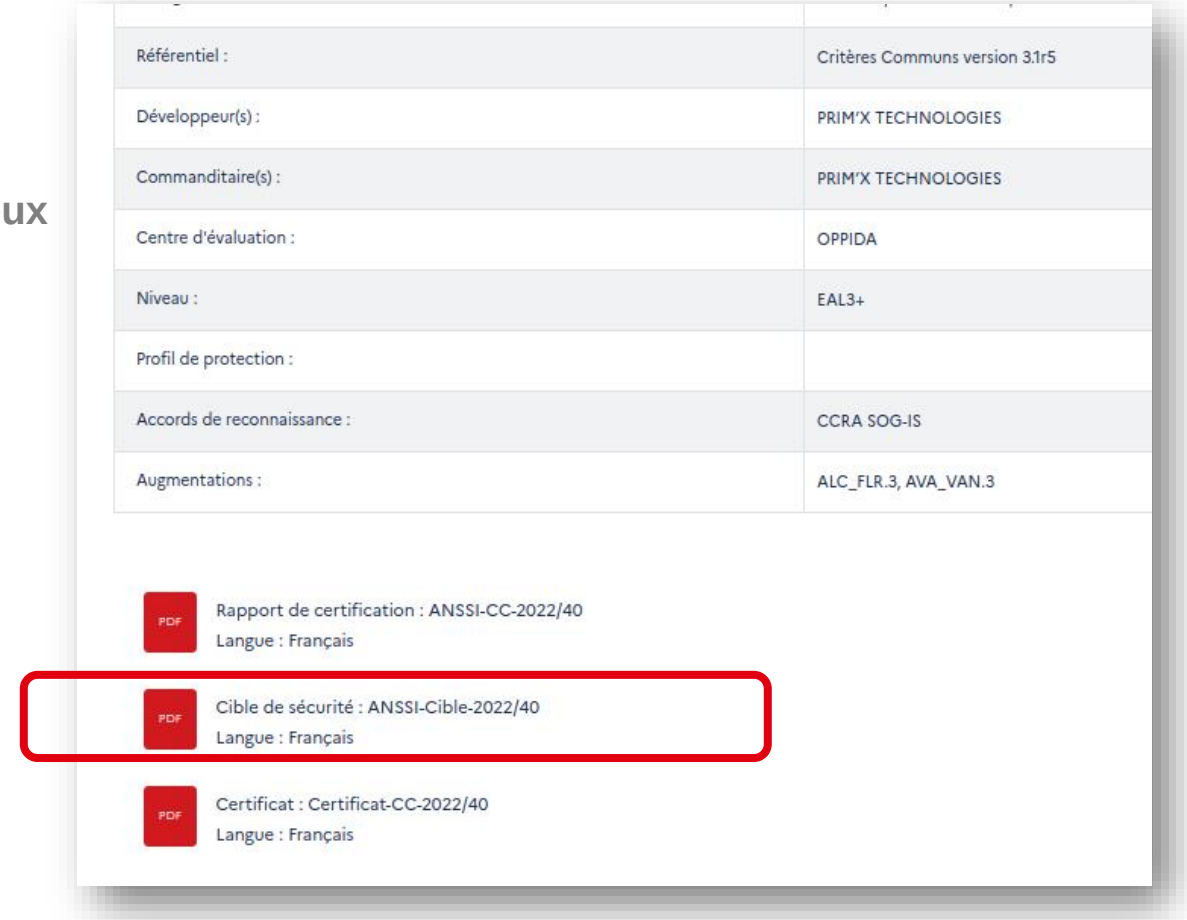
La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

# Agrément Zed!

## Le parcours du RSSI minutieux

5. Consultation des documents

- Cible de sécurité
- Conditions d'utilisation
- …



| | |
|---|---|
| Référentiel : | Critères Communs version 3.1r5 |
| Développeur(s) : | PRIM'X TECHNOLOGIES |
| Commanditaire(s) : | PRIM'X TECHNOLOGIES |
| Centre d'évaluation : | OPPIDA |
| Niveau : | EAL3+ |
| Profil de protection : | |
| Accords de reconnaissance : | CCRA SOG-IS |
| Augmentations : | ALC_FLR.3, AVA_VAN.3 |

PDF Rapport de certification : ANSSI-CC-2022/40
Langue : Français

PDF Cible de sécurité : ANSSI-Cible-2022/40
Langue : Français

PDF Certificat : Certificat-CC-2022/40
Langue : Français

# Agrément Zed!

## Le parcours du RSSI pointilleux

5. Consultation des documents

- Cible de sécurité
- Conditions d'utilisation
- …

C6. Pour chaque nouvel envoi, il est nécessaire de créer un nouveau conteneur chiffré.

- La politique P399 (version du format des conteneurs et messages chiffrés) doit être configurée à « Version 2 ».

C7. Afin de renforcer le contrôle d'intégrité, la politique P234 doit interdire l'ouverture de conteneurs ZED au format 2.2. A cet effet, elle doit être configurée en ajoutant la ligne « ZedFormatVersion2.2 | Deny ».

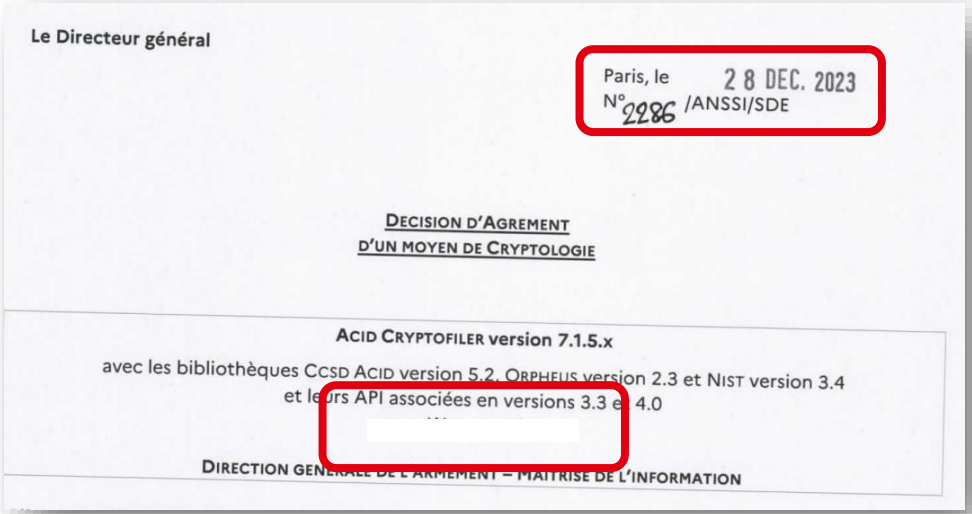
- La politique P730 (seuil d'acceptation des mots de passe) doit être configurée à 100% et la politique P732 (longueur des mots de passe) doit être configurée à 12.

# Agrément Acid

## Le parcours du RSSI pointilleux

5. Consultation des documents

- Cible de sécurité
- Conditions d'utilisation
- …



Le Directeur général

Paris, le 28 DEC. 2023
N° 2286 /ANSSI/SDE

DECISION D'AGREMENT
D'UN MOYEN DE CRYPTOLOGIE

ACID CRYPTOFILER version 7.1.5.x

avec les bibliothèques CCSD ACID version 5.2, ORPHEUS version 2.3 et NIST version 3.4
et leurs API associées en versions 3.3 et 4.0

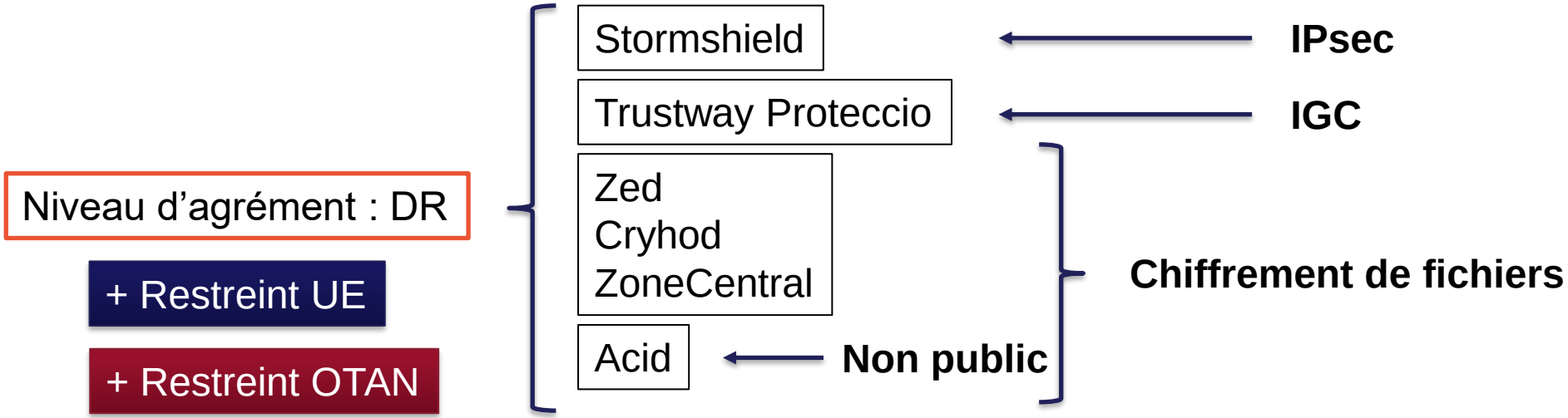
DIRECTION GENERALE DE L'ARMEMENT – MAITRISE DE L'INFORMATION

**Limites**

L1. Seule lutilisation d'ACID CRYPTOFILER sur l'OS Windows Seven est couverte par le présent agrément. Les utilisations sur les OS Windows XP, Windows Vista, Windows 8, Windows 10, Windows 11 et Windows Server ne sont pas couvertes par le présent agrément.

L2. L'usage de la fonction [illegible]

# Agrément pour le DR




https://cyber.gouv.fr/produits-services-qualifies

# Choix de la cible

## Intérêt

- Zed! : seul logiciel accessible à tous pour l'envoi et la réception d'information DR

- Il est donc :
  - Déployé chez la grande majorité des entreprises traitant de l'information sensible (DR)
  - « Exposé » à des canaux non sûrs (e-mails, clés USB, etc.)
  - Une « cible potentielle » en audit

- Agrément DR, donc Qualification de niveau « standard », donc Critère Communs EAL3+
  - Donc une cible de sécurité qui a été regardé (et d'autres travaux non spécifiés)
  - Mais qui ne couvre pas tout l'objet **en tant que logiciel**

# Choix de la cible

## Hypothèses de l’analyse

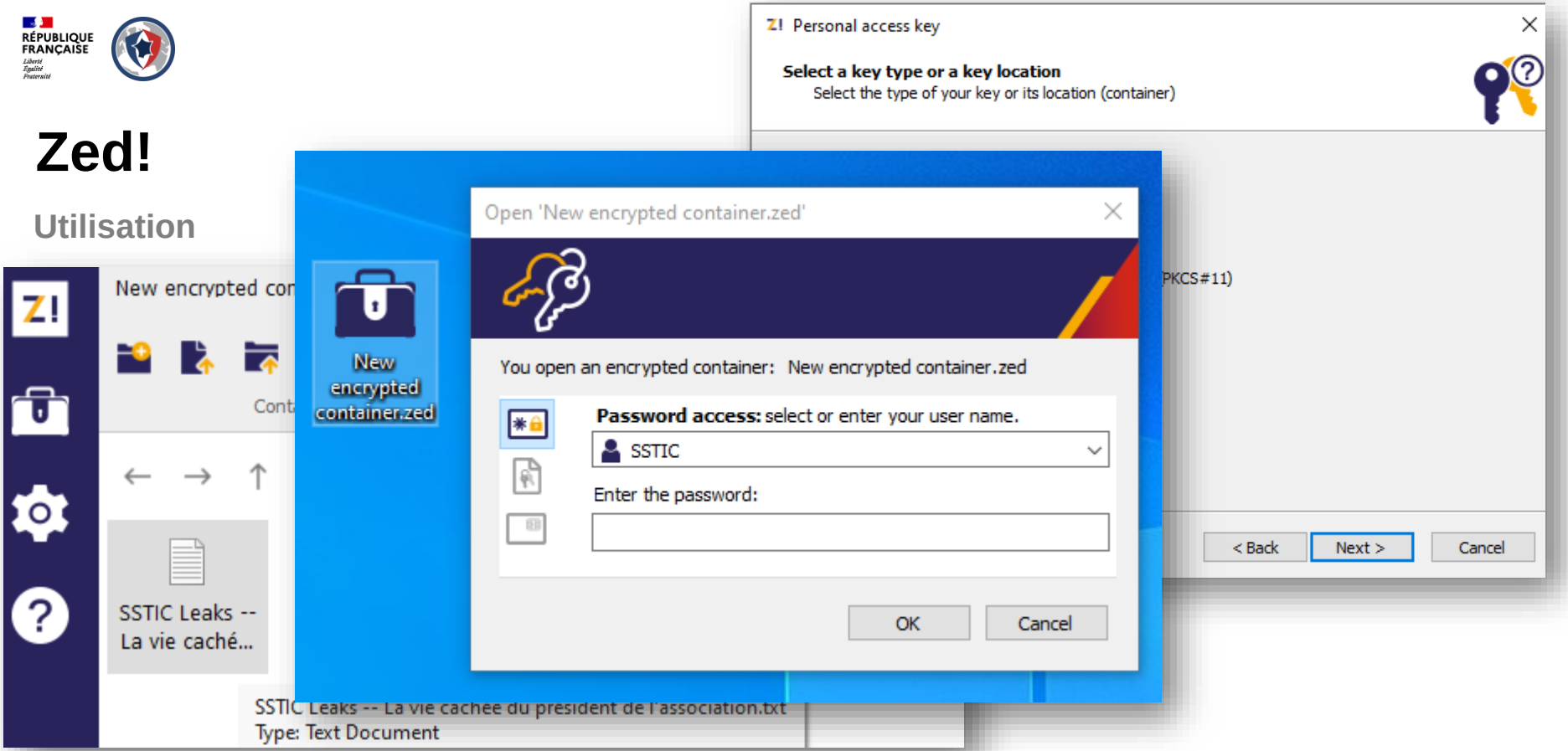
Représentativité d’un attaquant :

- Comme un client du produit
- Aucun accès à de l’information secrète

# 2. DÉMARCHE D’ANALYSE

# Zed!

## Utilisation




Tutoriel : https://spote.developpement-durable.gouv.fr/mtect-mte-mer/sg/sg-dnum/sg-dnum-msp/article/tuto-transmettre-des-documents-a-donnees-sensibles-grace-a-zed-et-france

# A. APPROCHE « BOITE NOIRE »

# Eléments disponibles en ligne

**Cible de sécurité**

- Cryptographie AES-256
- Utilisations possibles
- Eléments d'architecture

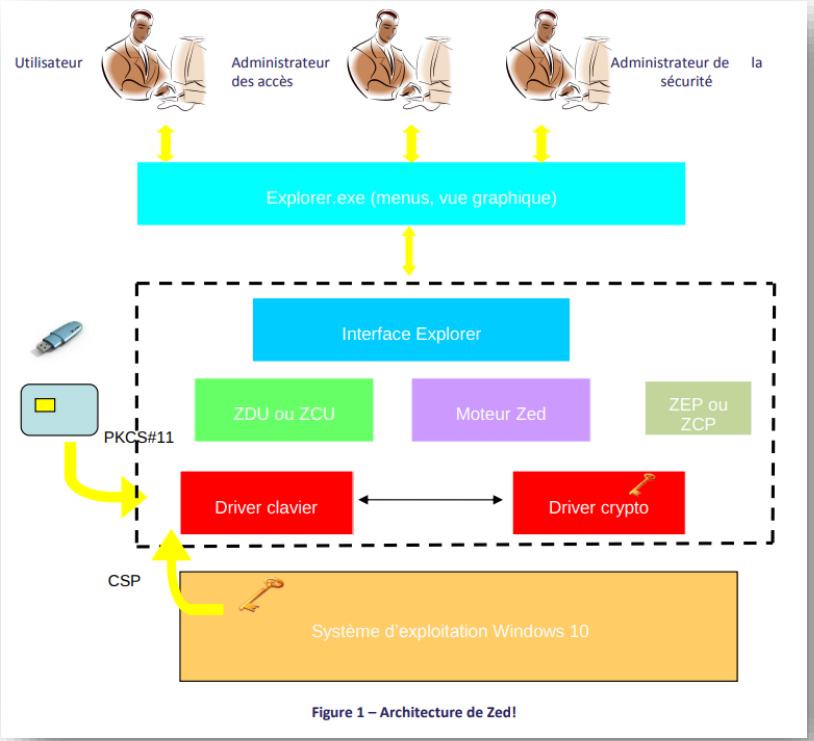
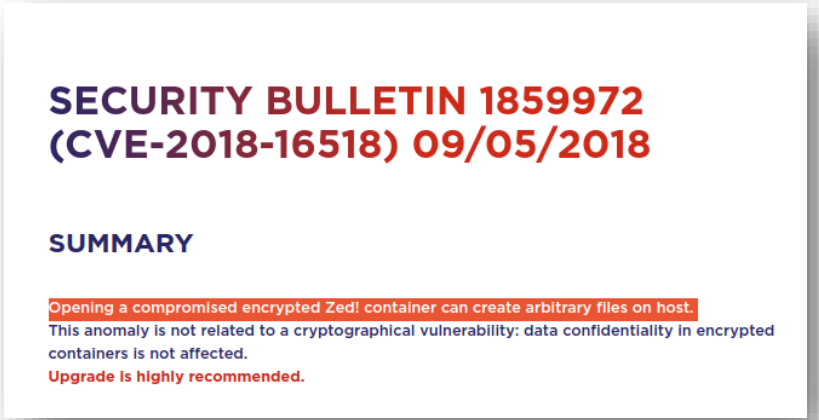



Figure 1 – Architecture de Zed!

https://cyber.gouv.fr/produits-certifies/zed-version-q20211

# Eléments disponibles en ligne

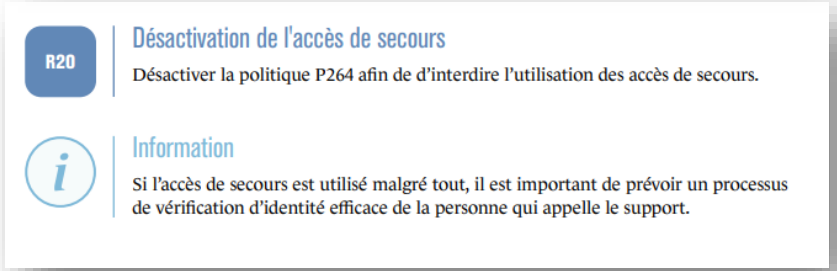
| | |
|---|---|
| Cible de sécurité | •Cryptographie AES-256<br>•Utilisations possibles<br>•Eléments d'architecture |
| Vulnérabilités | •CVE-2018-16518 (CVSS 8.3)<br>•« L'ouverture d'une archive peut créer des fichiers arbitraires » |




https://www.primx.eu/en/bulletins/security-bulletin-1859972/

# Eléments disponibles en ligne

| | |
|---|---|
| Cible de sécurité | •Cryptographie AES-256<br>•Utilisations possibles<br>•Eléments d'architecture |
| Vulnérabilités | •CVE-2018-16518 (CVSS 8.3)<br>•« L'ouverture d'une archive peut créer des fichiers arbitraires » |
| Guide ANSSI | •Accès de secours<br>•Extensions de fichier peuvent être clairs/cachées<br>•Chiffrement : mot de passe ou certificat |

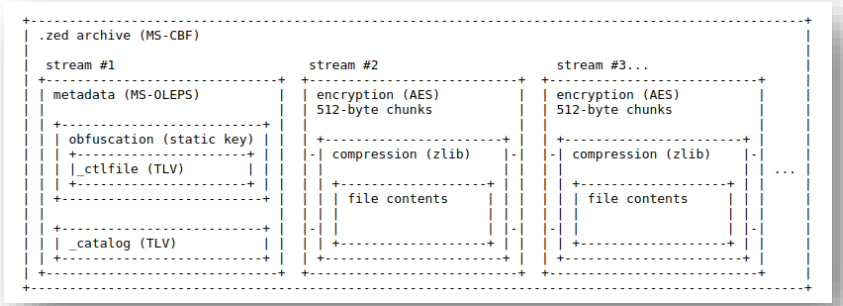





https://cyber.gouv.fr/publications/recommandations-pour-une-utilisation-securisee-de-zed

# Eléments disponibles en ligne

| | |
|---|---|
| Cible de sécurité | •Cryptographie AES-256<br>•Utilisations possibles<br>•Eléments d'architecture |
| Vulnérabilités | •CVE-2018-16518 (CVSS 8.3)<br>•« L'ouverture d'une archive peut créer des fichiers arbitraires » |
| Guide ANSSI | •Accès de secours<br>•Extensions de fichier peuvent être clairs/cachées<br>•Chiffrement : mot de passe ou certificat |
| Analyse du format Zed! (version antérieure) | •Format de base : MS-CFB (Office)<br>•Clé de chiffrement *hardcodée* pour obscurcir<br>•Données sous une forme TLV |




https://www.beuc.net/zed/

# Eléments disponibles en ligne

| | |
|---|---|
| Cible de sécurité | •Cryptographie AES-256<br>•Utilisations possibles<br>•Eléments d'architecture |
| Vulnérabilités | •CVE-2018-16518 (CVSS 8.3)<br>•« L'ouverture d'une archive peut créer des fichiers arbitraires » |
| Guide ANSSI | •Accès de secours<br>•Extensions de fichier peuvent être clairs/cachées<br>•Chiffrement : mot de passe ou certificat |
| Analyse du format Zed! (version antérieure) | •Format de base : MS-CFB (Office)<br>•Clé de chiffrement *hardcodée* pour obscurcir<br>•Données sous une forme TLV |
| Format JtR | •`zed2john.py`<br>•Dérivation des mots de passe |

john / run / **zed2john.py**

Code | Blame | Executable File · 140 lines (115 loc) · 4.47 KB

```
25
26  CTLFILE_DELIMITER = b'\x07\x65\x92\x1A\x2A\x07\x74\x53\x47\x52\x07\x33\x61\x71\x93\x00'
27  STATIC_KEY = b'\x37\xF1\x3C\xF8\x1C\x78\x0A\xF2\x6B\x6A\x52\x65\x4F\x79\x4A\xEF'
28  VER1 = b'\x01\x00'
29  VER2 = b'\x02\x00'
30  PBA_SALT = b'\x80\x7a\x05\x00'
31  PBA_ITER = b'\x80\x7b\x02\x00'
32  HASH_FUNC = b'\x80\x78\x02\x00'
33  PBA_CHK = b'\x80\x79\x05\x00'
34
35  USERNAME = b'\x80\x71\x04\x00'
36
37  PY3 = sys.version_info[0] == 3
38
39  if not PY3:
40      reload(sys)
41      sys.setdefaultencoding("utf8")
```

*An intermediary user key, a user IV and an integrity check*
*sum will be derived from the user password, using the **deprecated PKCS#12** method as described at **rfc7292 appendix B***

https://github.com/openwall/john/blob/bleeding-jumbo/run/zed2john.py

# Observations initiales

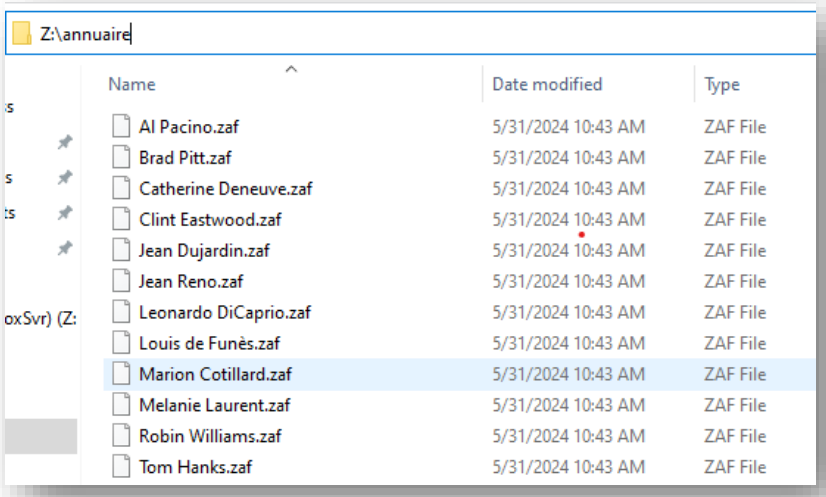
## Stockage des listes d'accès

https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

- *ProcMon* pour observer les lectures de fichier
- Création d'une clé privée

  → `NOM_UTILISATEUR.zaf` créé puis accédé
- Suppression de tous les fichiers `.zaf`

  → le programme redemande de créer une clé

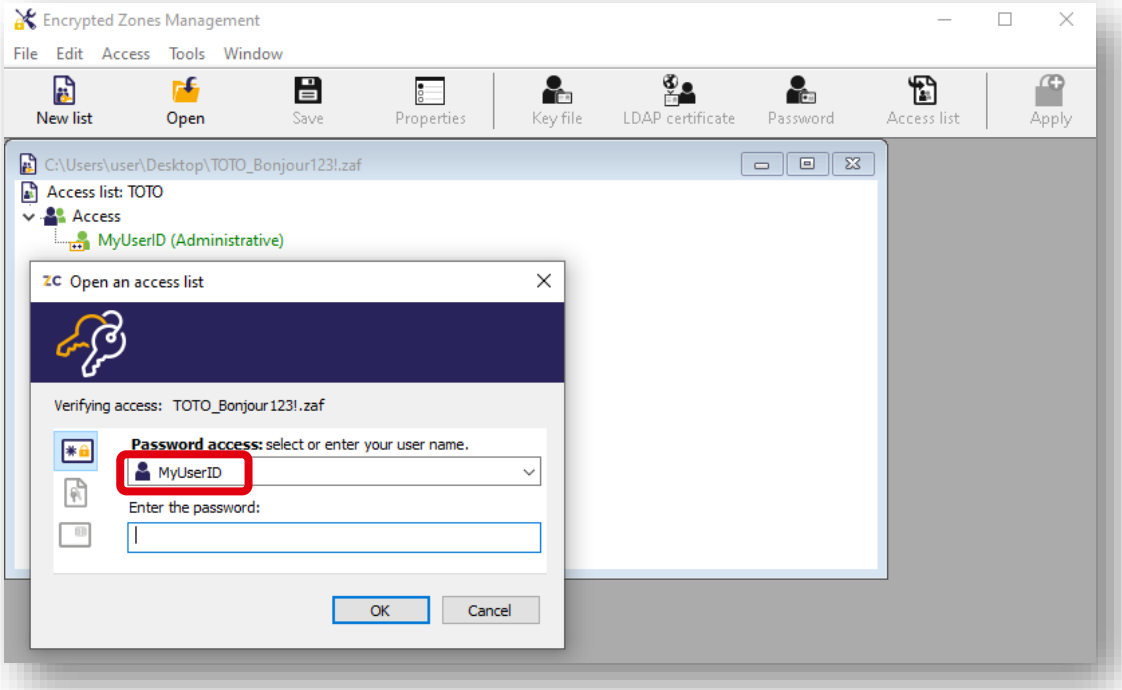



`.zaf` : correspond ou contient au moins la clé privée de l'utilisateur

# Observations initiales

## Format

- Ouverture dans l'outil de gestion *Encrypted Zone Management*
- Absence de chaînes de caractères dans le fichier
- Entropie (`binwalk -E`) proche de 1




`.zaf` : probablement compressé ou chiffré

# Observations initiales

## Emport de la clé de déchiffrement


1. Création d'un compte `MyUser`
2. Création d'une archive Zed!
3. Ouverture et utilisation de l'archive

4. Ouverture de l'archive
5. Le compte `MyUser` est disponible et fonctionnel !

→ Fichier `MyUser.zaf` non nécessaire sur la destination

→ Une archive Zed! **emporte** le moyen d'être déchiffrée (au moins le compte créateur)

# B. ANALYSE DU ZAF

# Analyse statique

## Rétro-ingénierie

- Plusieurs plateformes et éditions
  - Linux, Windows, …
  - Free, Commercial, …
- Binaires volumineux, a priori C++
  - Notoirement fastidieux
- Utilisation de cryptographie
  - Plugins (*FindCrypt*, …)
  - Accélération matérielle (instructions AES-NI)
  - Instructions typique de certains algorithmes, ex: HMAC

Identification de plusieurs fonctions de cryptographie

```
XOR xxx, 0x5c
XOR xxx, 0x36
```

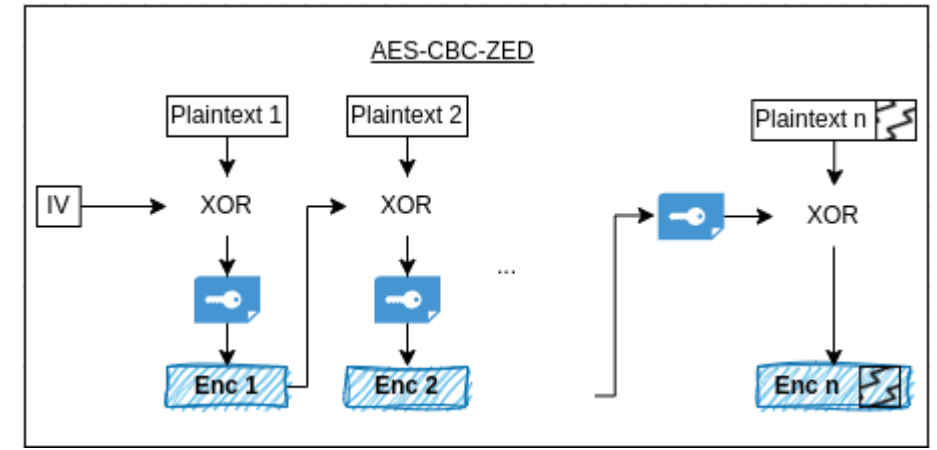
# Analyse dynamique

## Suivi du flot de donnée

# Analyse statique / dynamique

**Déchiffrement :**

- ✔ Algorithme : AES
- ✔ Mode
- ✔ *Padding*
- Secrets

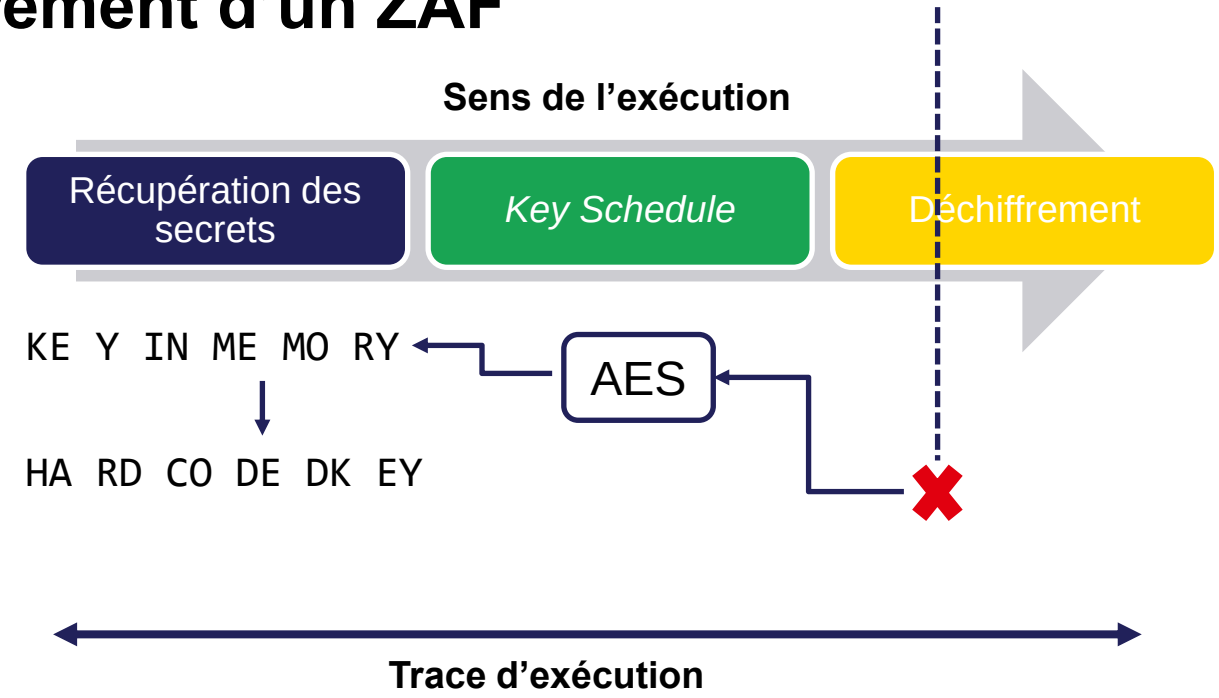



*Si partie CBC identique:*

$XOR(chiffrés_{CFB}) = XOR(clairs_{CFB})$

# Déchiffrement d’un ZAF

Secrets

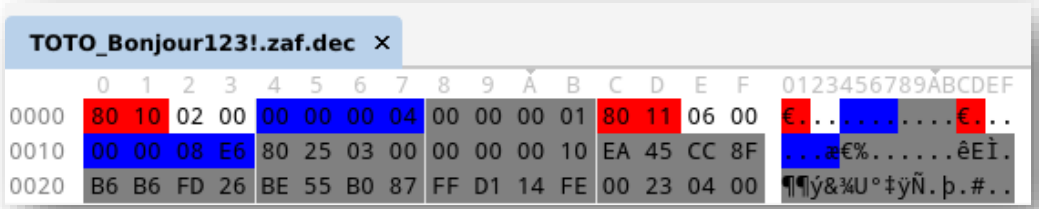



https://aka.ms/ttd

Linux : `rr`

# Contenu d'un ZAF

## Post analyse




**Déchiffrement**
- Clé *hardcodée*

**_Parsing_ du format**
- TLV

**Contenu**
- *Username*, privilèges, …
- Emails + alias
- SID et DN de l'utilisateur
- Si PKI, certificat associé
- Clé publique RSA
- [Secrets chiffrés]

```
c.mougey@sstic.org
user123@sstic.org
office365@onmicrosoft.com
```

```
S-1-5-21-XXX-YYY-ZZZ-1234
CN=CamilleM,OU=Users,DC=sstic,DC=org
```

# Contenu d’un ZAF

## Déchiffrement du secret

### RFC 7292, Appendix B

- Authentification : *password* → `ID 1` + 200 000 `SHA-256` → 8 premiers octets
- Déchiffrement :
  - *password* → `ID 2` + 100 000 `SHA-256` → IV
  - *password* → `ID 3` + 100 000 `SHA-256` → Key

# Contenu d'un ZAF

## Format John-the-Ripper

```
user@user-laptop:~/etudes/binaries/ZoneCentral$ python3.8 read_zaf.py --quiet --john TOTO_Bonjour123\!.zaf | tee /tmp/to_crack
MyUserID:$zed$1$22$200000$71fc1704150d6bdcbd94b3d3c7592c87$df0ff55ba8084781:::TOTO_Bonjour123!.zaf
user@user-laptop:~/etudes/binaries/ZoneCentral$ ~/tools/john/run/john /tmp/to_crack -w=/tmp/wordlist --skip-self-tests
Using default input encoding: UTF-8
Loaded 1 password hash (zed, Prim'X Zed! encrypted archives [PKCS#12 PBE (SHA1/SHA256) 256/256 AVX2 8x])
Cost 1 (iteration count) is 200000 for all loaded hashes
Cost 2 (hash-func [21:SHA1 22:SHA256]) is 22 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Warning: Only 1 candidate buffered, minimum 32 needed for performance.
Bonjour123!      (MyUserID)
1g 0:00:00:00 DONE (2023-08-11 11:08) 7.692g/s 7.692p/s 7.692c/s 7.692C/s Bonjour123!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

4 cœurs i5-7200U

200 essais / secondes

Si un attaquant accède à un `.zaf`, il peut essayer de trouver le secret
Faisabilité : seulement des attaques par dictionnaire

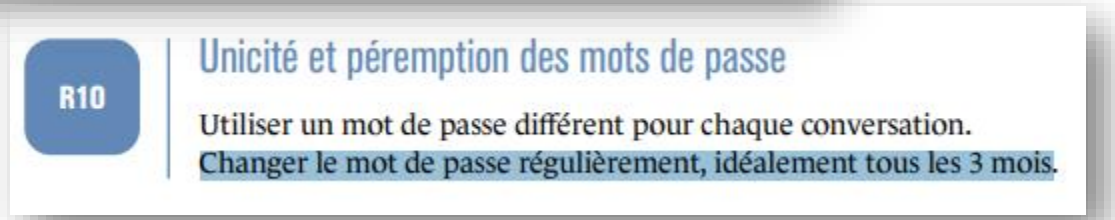
# ZAF

P383, P386, P387 et P233), il faut ajouter les politiques ZoneCentral suivantes (qui s'appliquent à la création de la liste d'accès de l'utilisateur) :

- La politique P702 (durée de validité des mots de passe) doit être configurée à une valeur inférieure à 90 jours.

## Autres remarques

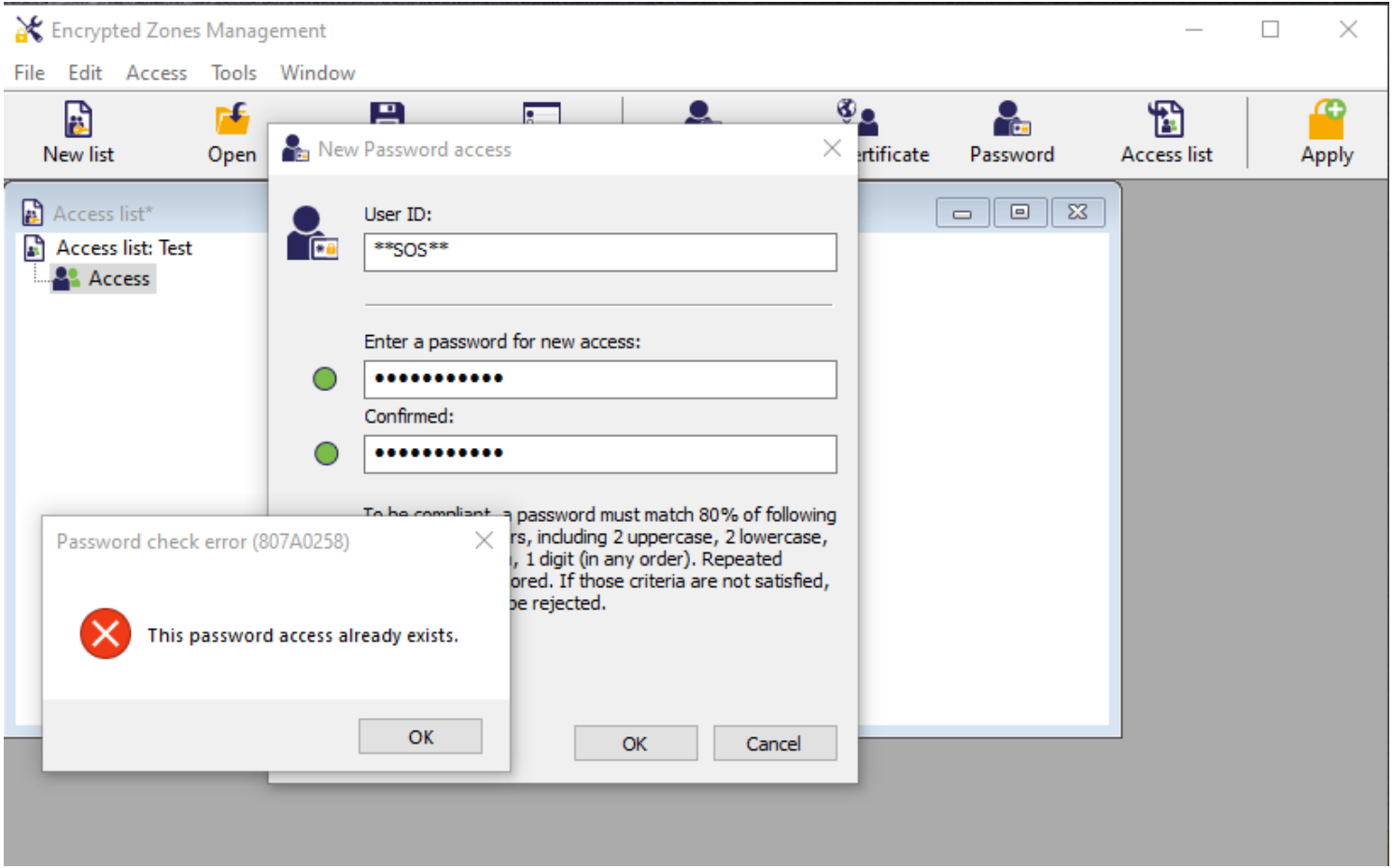
- Le vrai secret est la clé privée du ZAF



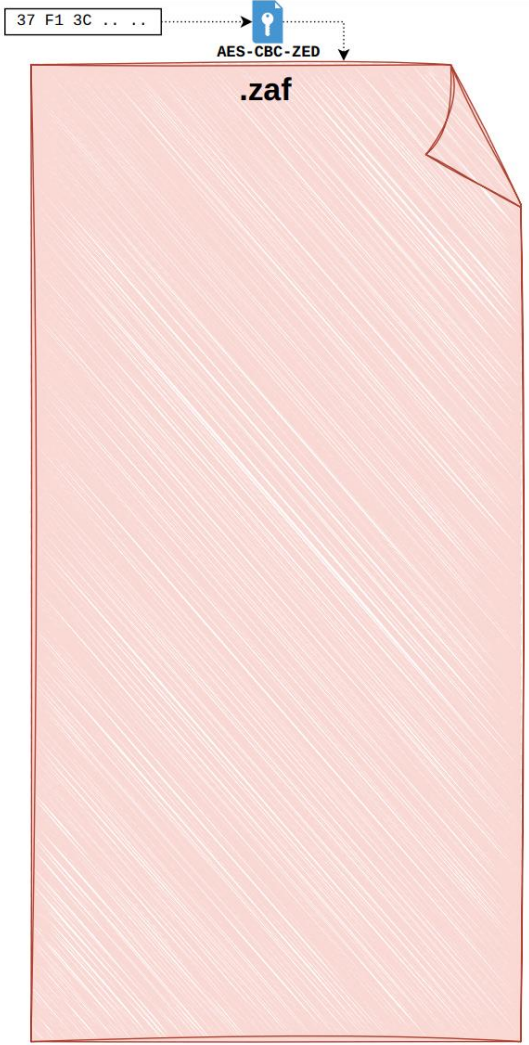

- Possibilité d'avoir plusieurs comptes dans le même ZAF
  - Souvent, chaîne « sécurité des données »
- Un compte caché **SOS** existe
  - Compte de secours
  - Son mot de passe (aléatoire) est chiffré avec la clé globale du ZAF
  - Récupérable par un utilisateur / administrateur connaissant le secret du ZAF

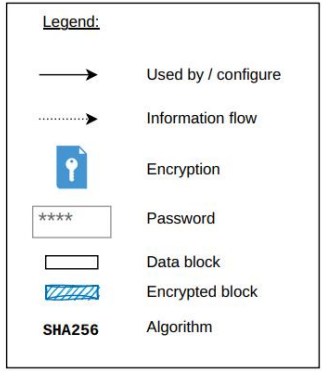
# ZAF

****SOS****

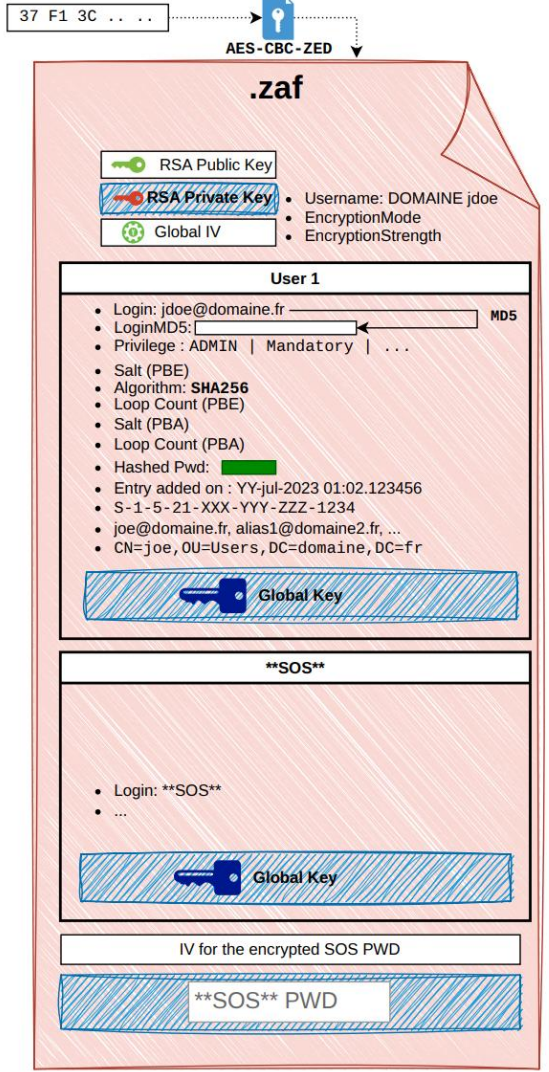

Encrypted Zones Management
File Edit Access Tools Window
New list
Open
Password
Access list
Apply
Access list*
Access list: Test
Access
New Password access
User ID:
**SOS**
Enter a password for new access:
Confirmed:
password must match 80% of following
rs, including 2 uppercase, 2 lowercase,
, 1 digit (in any order). Repeated
ored. If those criteria are not satisfied,
e rejected.
OK
Cancel
Password check error (807A0258)
This password access already exists.
OK

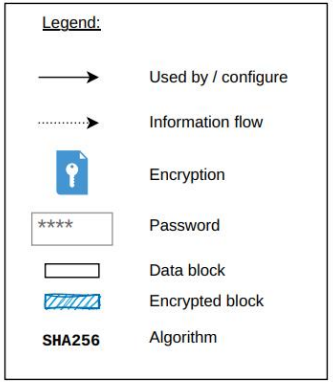
# ZAF


37 F1 3C .. ..
AES-CBC-ZED
.zaf

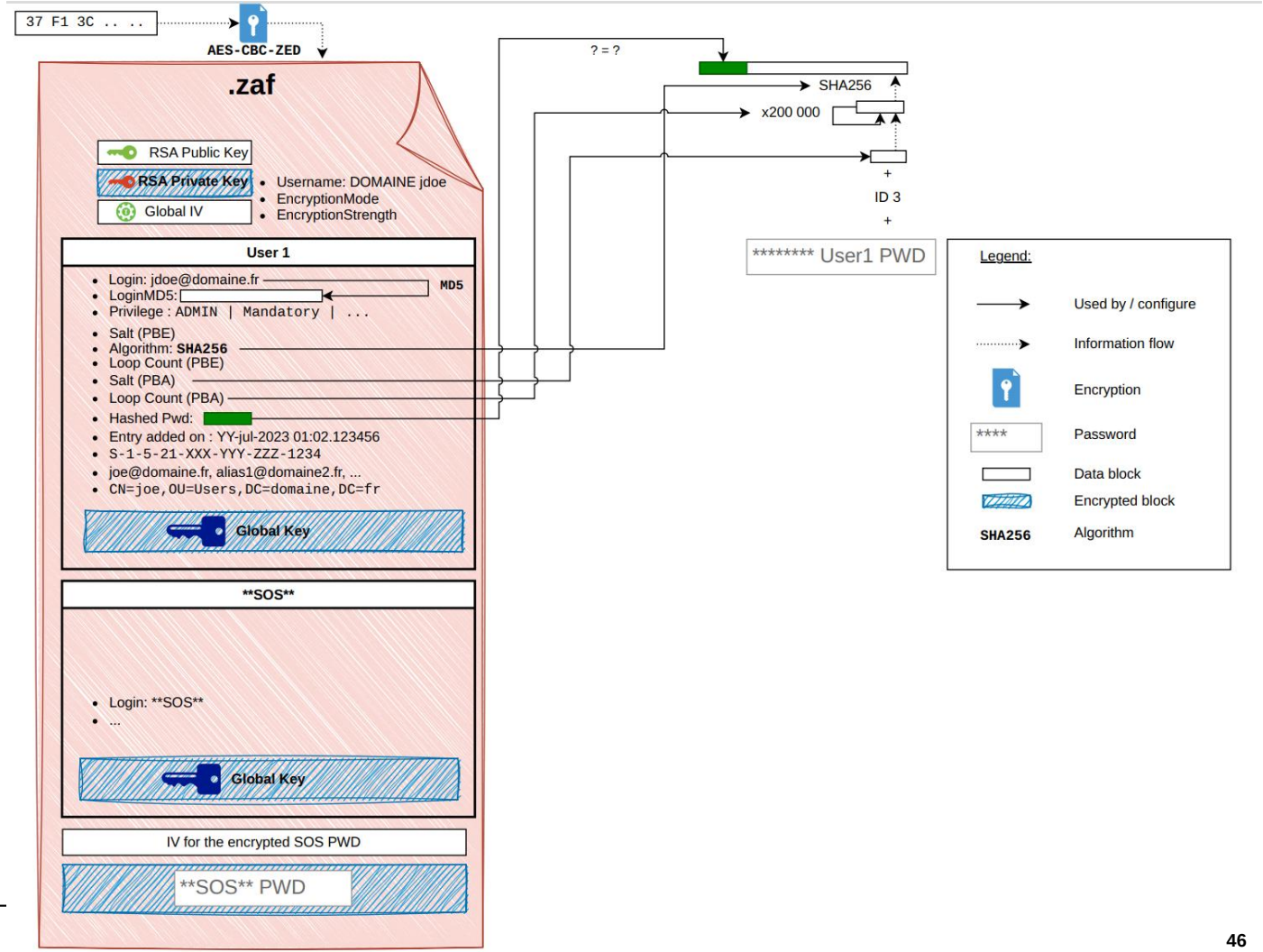

Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

# ZAF

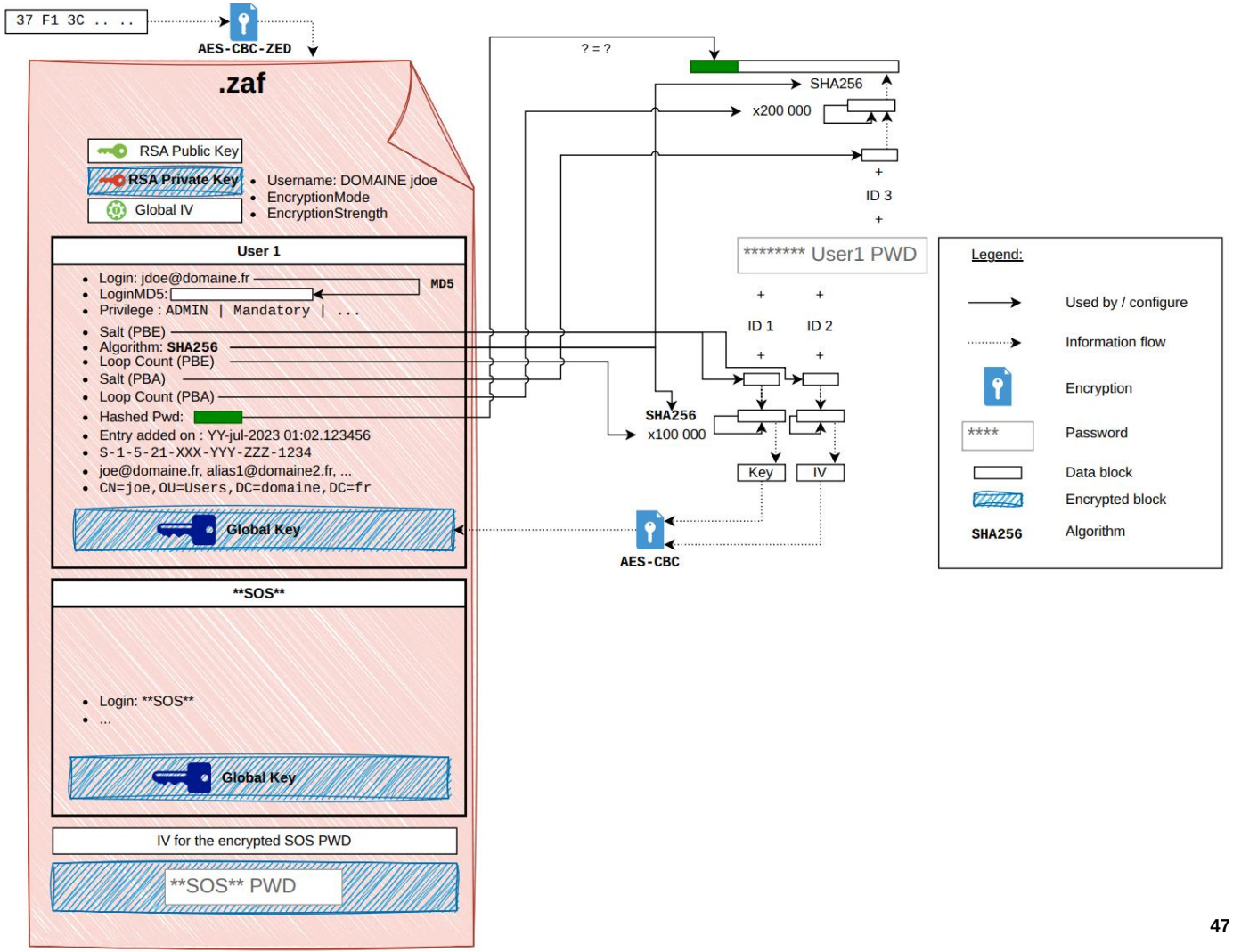

37 F1 3C .. ..
AES-CBC-ZED
.zaf
RSA Public Key
RSA Private Key
Global IV
Username: DOMAINE jdoe
EncryptionMode
EncryptionStrength
User 1
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
S-1-5-21-XXX-YYY-ZZZ-1234
joe@domaine.fr, alias1@domaine2.fr, ...
CN=joe,OU=Users,DC=domaine,DC=fr
Global Key
**SOS**
Login: **SOS**
...
Global Key
IV for the encrypted SOS PWD
**SOS** PWD


Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

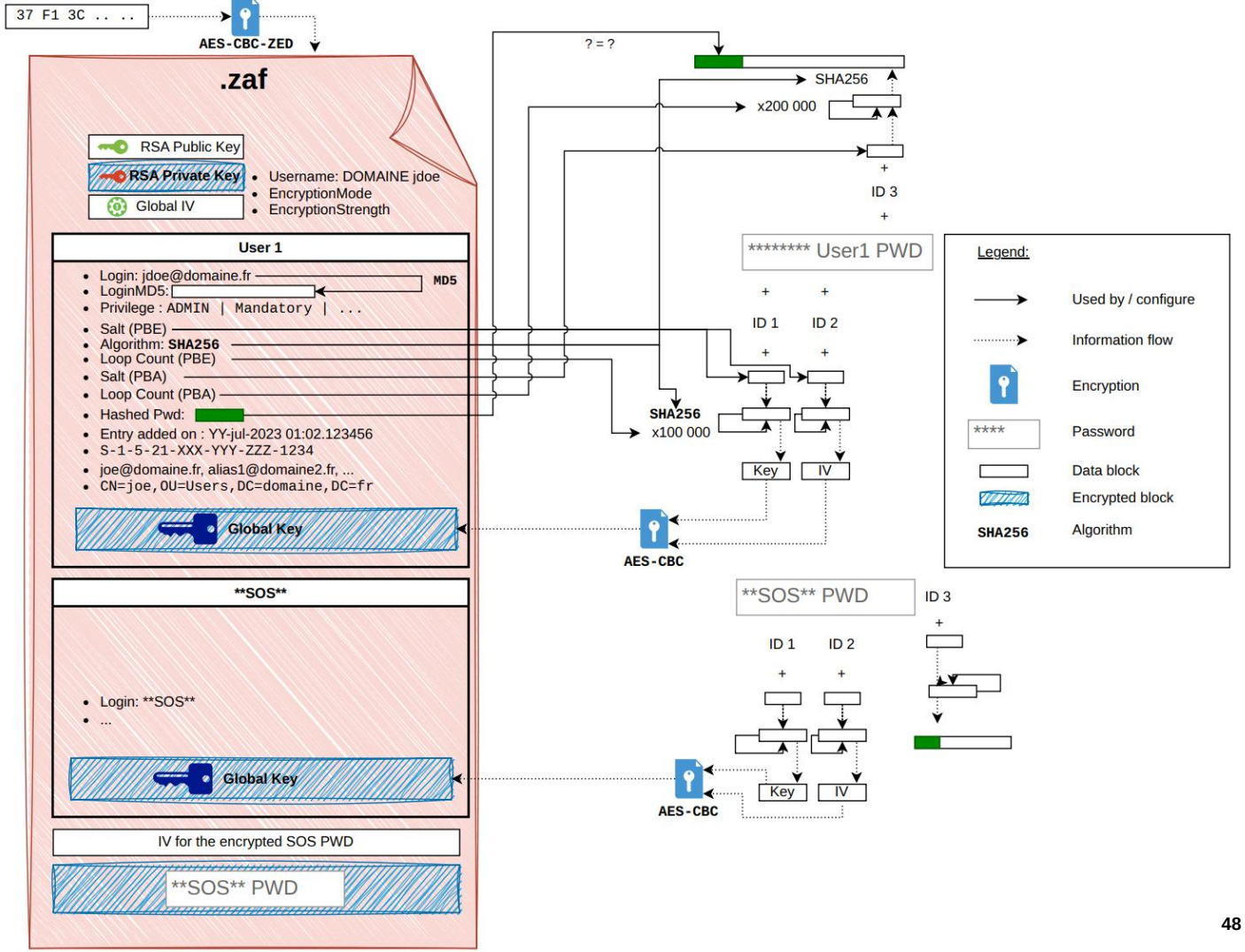
# ZAF


37 F1 3C .. ..
AES-CBC-ZED
.zaf
RSA Public Key
RSA Private Key
Global IV
Username: DOMAINE jdoe
EncryptionMode
EncryptionStrength
User 1
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
S-1-5-21-XXX-YYY-ZZZ-1234
joe@domaine.fr, alias1@domaine2.fr, ...
CN=joe,OU=Users,DC=domaine,DC=fr
Global Key
**SOS**
Login: **SOS**
...
Global Key
IV for the encrypted SOS PWD
**SOS** PWD
? = ?
SHA256
x200 000
+
ID 3
+
******** User1 PWD
Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

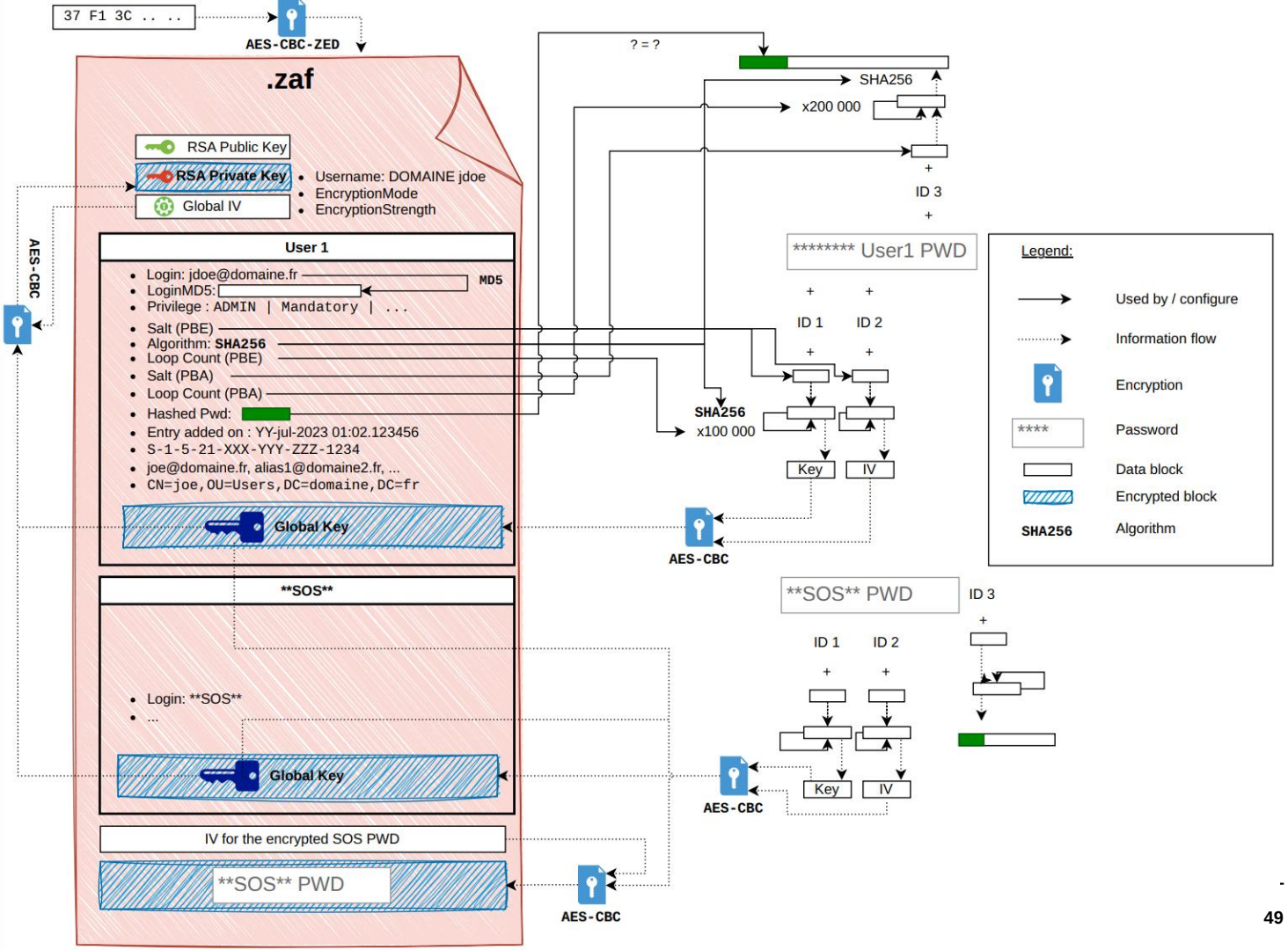
# ZAF


37 F1 3C .. ..
AES-CBC-ZED
.zaf
RSA Public Key
RSA Private Key
Global IV
Username: DOMAINE jdoe
EncryptionMode
EncryptionStrength
User 1
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
S-1-5-21-XXX-YYY-ZZZ-1234
joe@domaine.fr, alias1@domaine2.fr, ...
CN=joe,OU=Users,DC=domaine,DC=fr
Global Key
**SOS**
Login: **SOS**
...
Global Key
IV for the encrypted SOS PWD
**SOS** PWD
? = ?
SHA256
x200 000
ID 3
******** User1 PWD
ID 1
ID 2
SHA256
x100 000
Key
IV
AES-CBC
Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

# ZAF


37 F1 3C .. ..
AES-CBC-ZED
.zaf
RSA Public Key
RSA Private Key
Global IV
Username: DOMAINE jdoe
EncryptionMode
EncryptionStrength
User 1
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
S-1-5-21-XXX-YYY-ZZZ-1234
joe@domaine.fr, alias1@domaine2.fr, ...
CN=joe,OU=Users,DC=domaine,DC=fr
Global Key
**SOS**
Login: **SOS**
...
Global Key
IV for the encrypted SOS PWD
**SOS** PWD
? = ?
SHA256
x200 000
ID 3
******** User1 PWD
ID 1
ID 2
SHA256
x100 000
Key
IV
AES-CBC
**SOS** PWD
ID 3
ID 1
ID 2
Key
IV
AES-CBC
Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

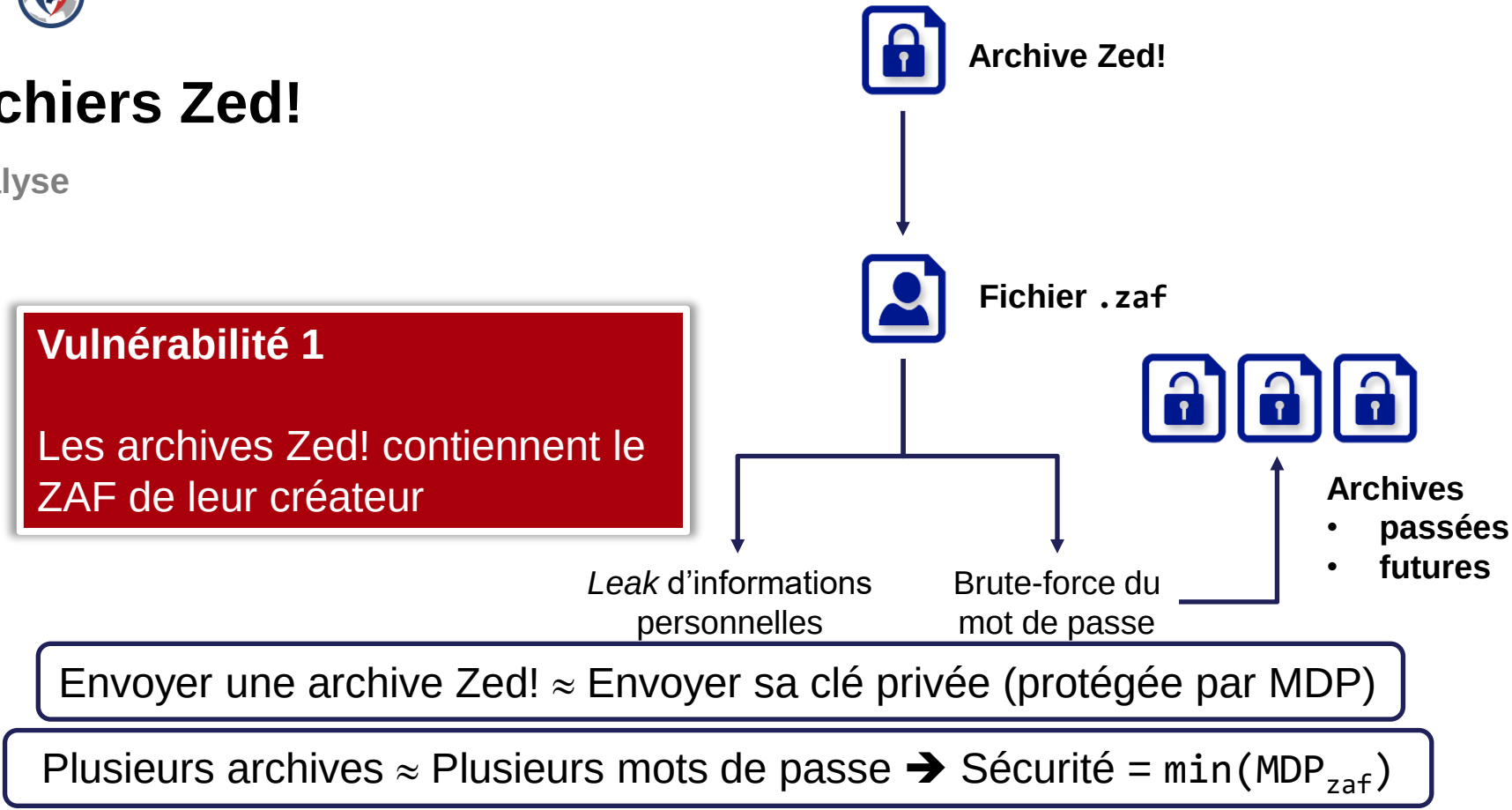
# ZAF


37 F1 3C .. ..
AES-CBC-ZED
.zaf
RSA Public Key
RSA Private Key
Global IV
Username: DOMAINE jdoe
EncryptionMode
EncryptionStrength
AES-CBC
User 1
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
S-1-5-21-XXX-YYY-ZZZ-1234
joe@domaine.fr, alias1@domaine2.fr, ...
CN=joe,OU=Users,DC=domaine,DC=fr
Global Key
**SOS**
Login: **SOS**
...
Global Key
IV for the encrypted SOS PWD
**SOS** PWD
AES-CBC
? = ?
SHA256
x200 000
ID 3
******** User1 PWD
ID 1
ID 2
SHA256
x100 000
Key
IV
AES-CBC
**SOS** PWD
ID 3
ID 1
ID 2
Key
IV
AES-CBC
Legend:
Used by / configure
Information flow
Encryption
****
Password
Data block
Encrypted block
SHA256
Algorithm

# C. FICHIERS ZED

# Fichiers Zed!

## Analyse




**Vulnérabilité 1**

Les archives Zed! contiennent le ZAF de leur créateur

Envoyer une archive Zed! ≈ Envoyer sa clé privée (protégée par MDP)

Plusieurs archives ≈ Plusieurs mots de passe ➔ Sécurité = $\texttt{min}(\texttt{MDP}_{\texttt{zaf}})$

# Fichiers Zed!

## Analyse

**Archive Zed!**

`X:\PartagesSecret\IncidentSSTIC\archive.zed`

**Vulnérabilité 2**

Une archive Zed! contient le « chemin initiale de création »

Comment vérifier tout ça ?

# Fichiers Zed!

CTI VIRUSTOTAL

CN = Requisition Judiciaire

Entreprise : [redacted]

M:\str-hfds-planification\04 - Planification\VIGIPIRATE\POSTURE ETE - AUTOMNE 2023\[redacted]

[redacted] Strasbourg - Audit PASSI LPM[redacted] 2023 - Procès Verbal de réception[redacted]

C:\Users\[redacted]\Documents\GMR_UKRAINE\GM60[redacted]

X:\[redacted]\Pole de compétence SYSTEMES DE COMBAT\[redacted]\3 – PROGRAMMES[redacted]

H:\ANALYSES DE LA MENACE ET AUTRES DOCS ENVOYES AUX OPERATEURS\CAMPAGNE DE SIGNALEMENT [redacted] 2021\[redacted]

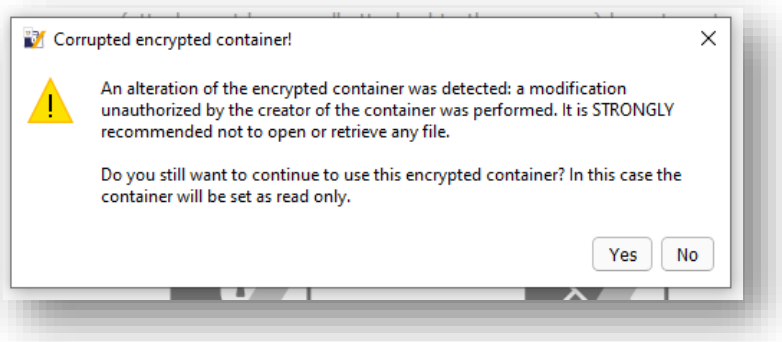

Fichier .zaf

**DN, SID, nom du domaine ANSSI**
**Adresses e-mails « anonymisées »**
**Si le mot de passe est BF…**

# Intégrité des archives

## Méthode



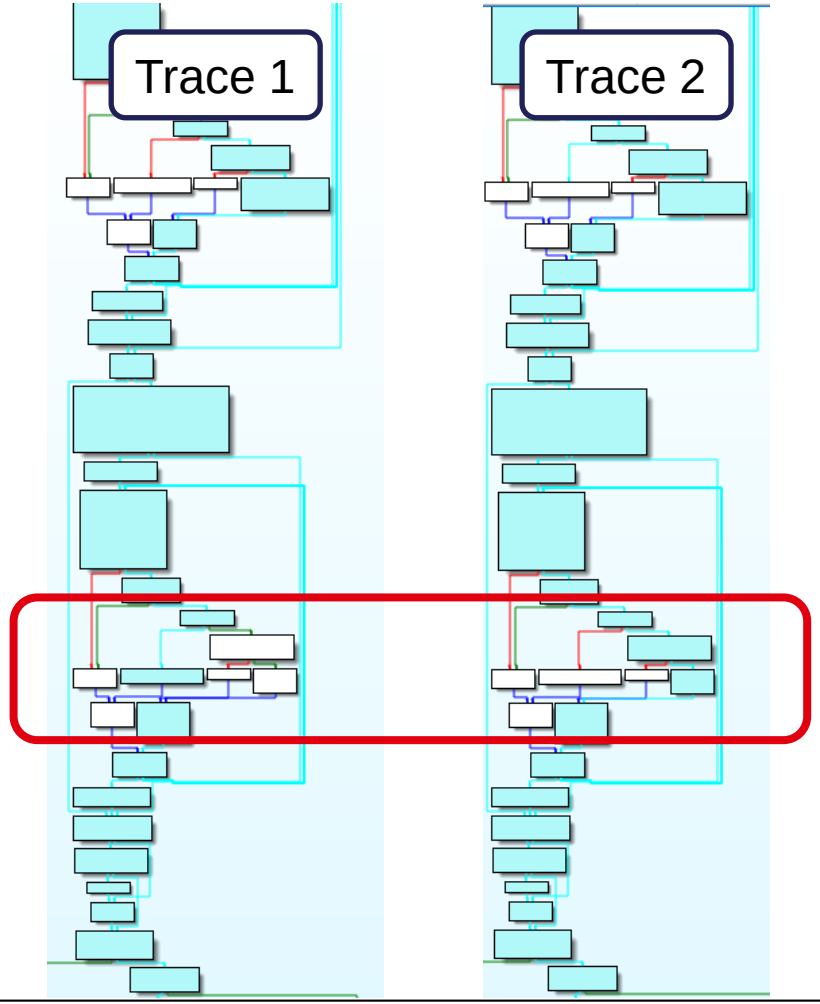


# Intégrité des archives

**Méthode: *diffing* de trace**

https://github.com/commial/ttd-bindings

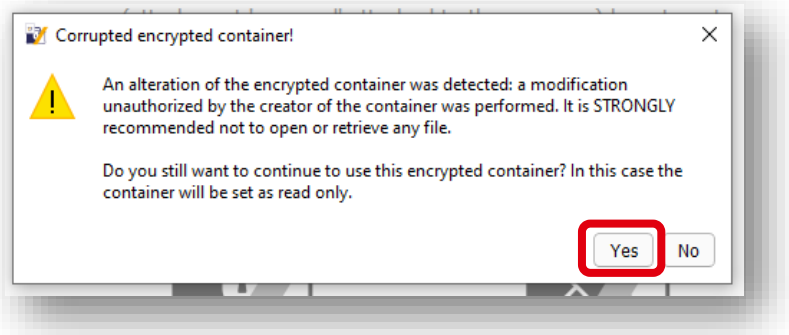
Permet d'isoler directement le code responsable



# Intégrité des archives

**Remarque 2**

Suppression du HMAC → Perte d'intégrité des fichiers
*Warning*, mais l'utilisateur peut accepter



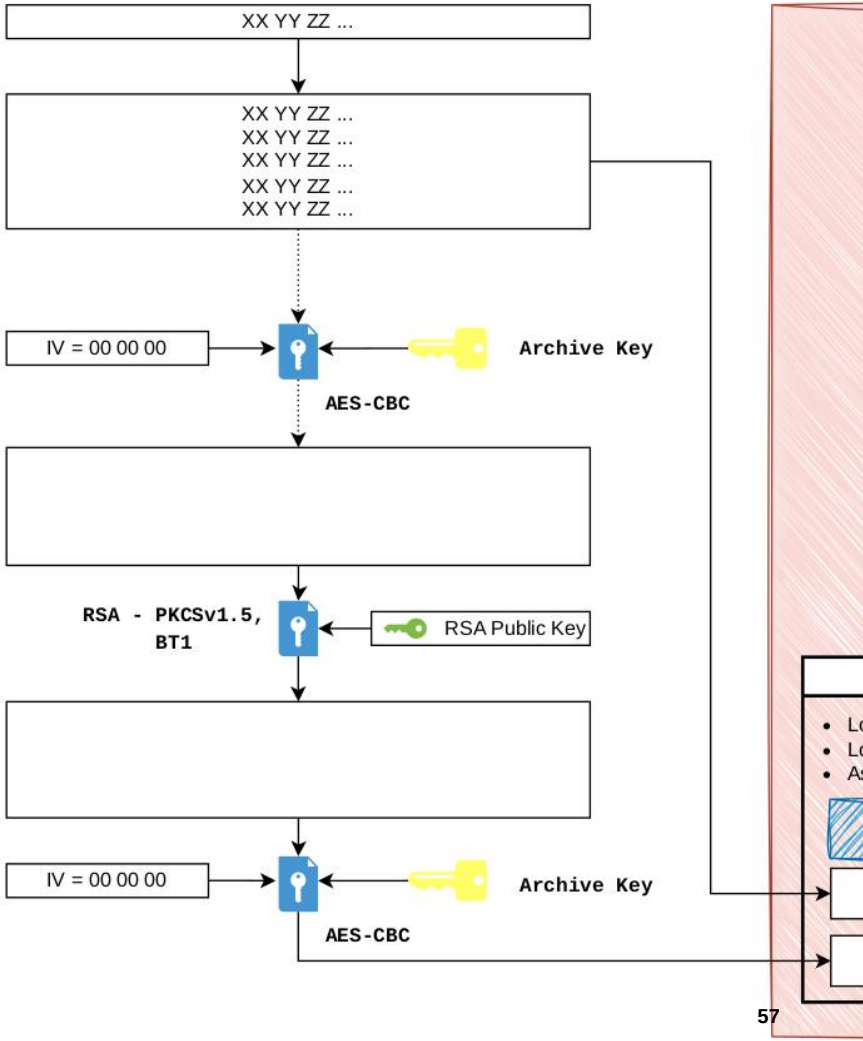
# Champs mystères

## Étapes :

1. `0x10` octets
2. Répétés n fois
3. Copié dans l'archive
4. Chiffrés
   `AES-CBC(IV=0, key=ArchiveKey)`
5. Re-chiffrés
   `RSA(PKCSv1.5, key=ArchivePubKey)`
6. Re-re-chiffrés
   `AES-CBC(IV=0, key=ArchiveKey)`
7. Copié dans l'archive

À quoi sert ce schéma ?

Ces octets sont-ils de la donnée ?

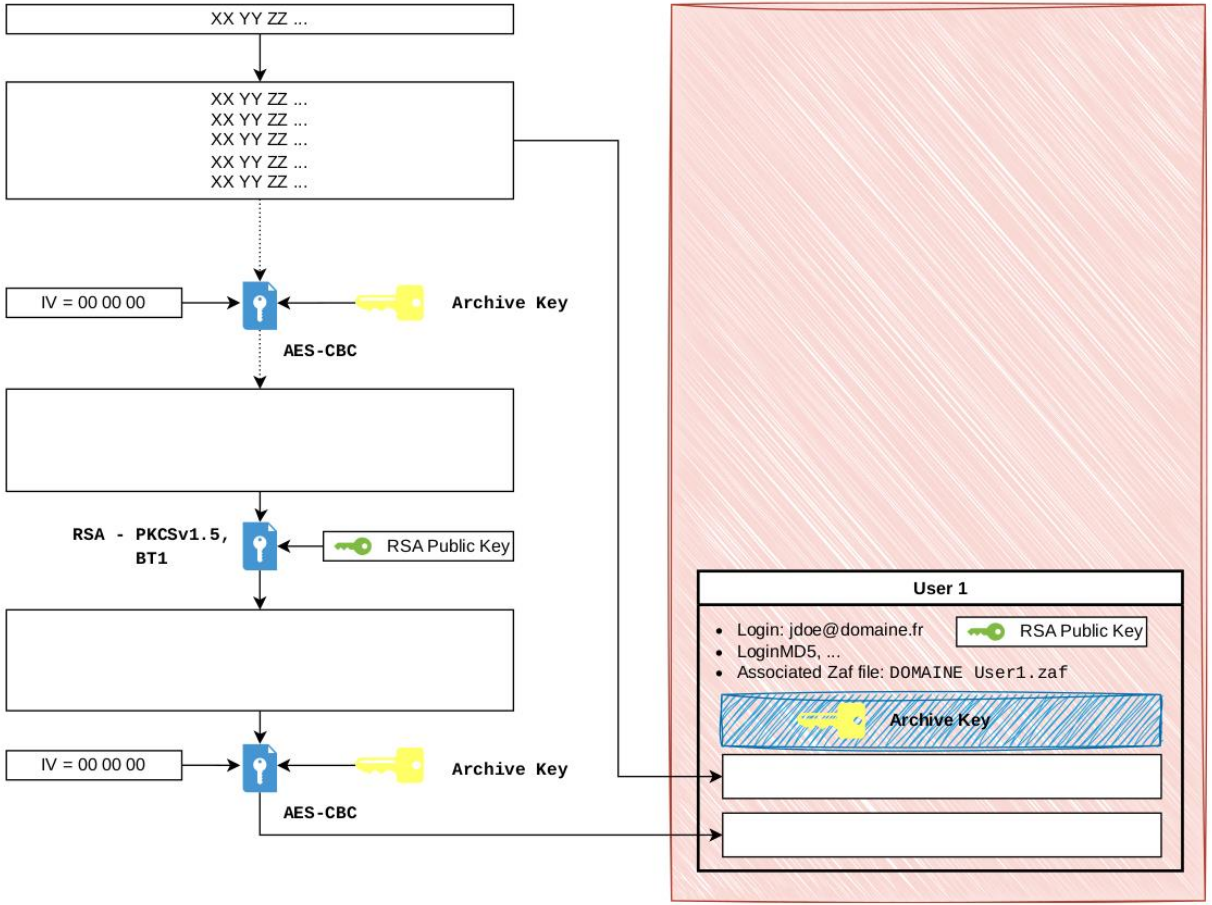


# Champs mystères

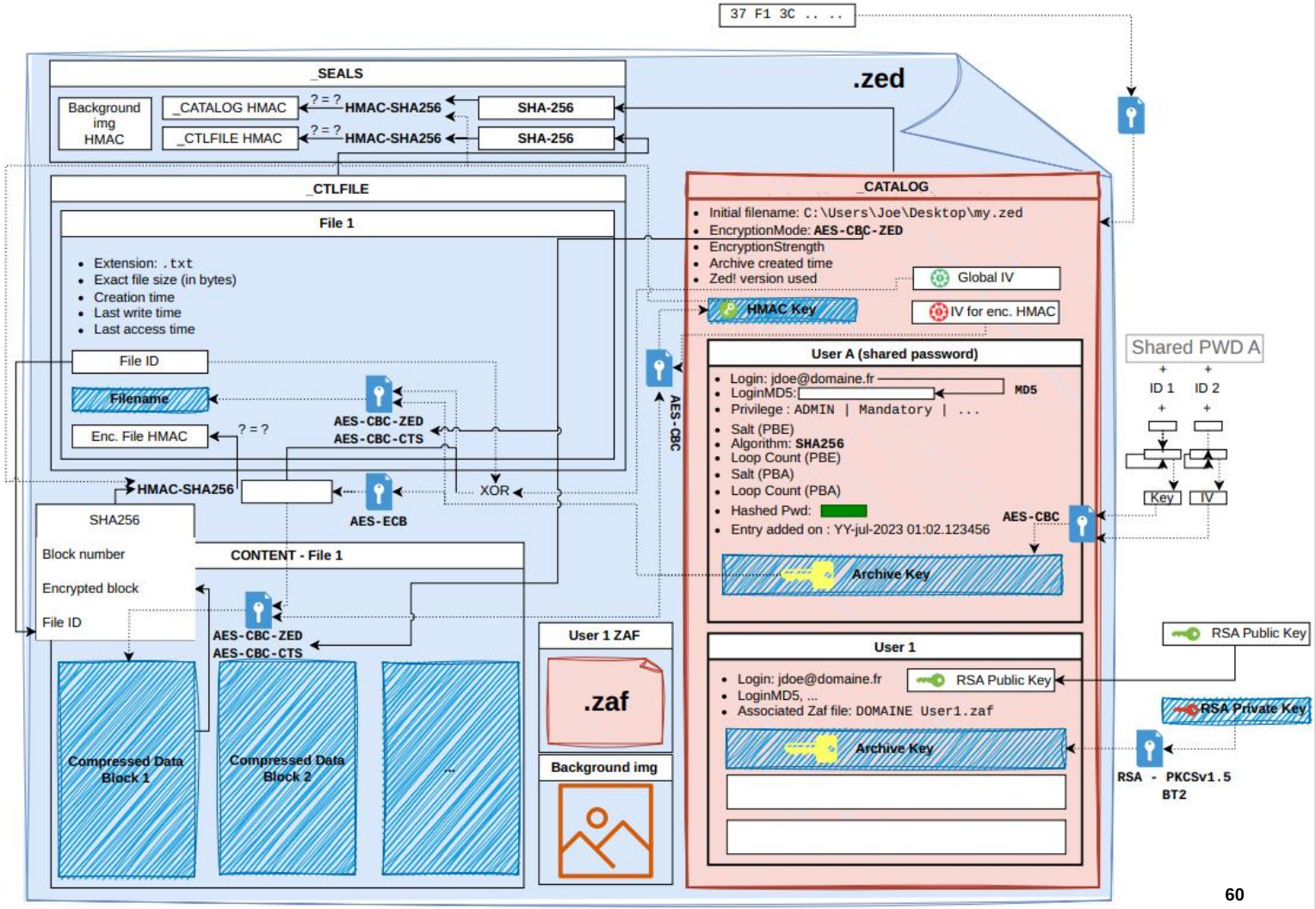
*Spoiler :*

- Code de manipulation de *BigNum*
- Emulation symbolique (`Miasm`) pour découvrir automatiquement les opérations
- Emulation des opérations de plus haut niveau → équations
- Hyperelliptic.org
- Dual EC-DRBG en *x-only*
- Non utilisé dans le « vrai » code
- Reliquat, peut-être pour vérifier lors du re-chiffrement d'une archive

Détails dans les actes



# Zed


37 F1 3C .. ..
.zed
_SEALS
Background img HMAC
_CATALOG HMAC
_CTLFILE HMAC
? = ?
HMAC-SHA256
SHA-256
_CTLFILE
File 1
Extension: .txt
Exact file size (in bytes)
Creation time
Last write time
Last access time
File ID
Filename
Enc. File HMAC
AES-CBC-ZED
AES-CBC-CTS
HMAC-SHA256
AES-ECB
XOR
SHA256
Block number
Encrypted block
File ID
CONTENT - File 1
Compressed Data Block 1
Compressed Data Block 2
...
User 1 ZAF
.zaf
Background img
_CATALOG
Initial filename: C:\Users\Joe\Desktop\my.zed
EncryptionMode: AES-CBC-ZED
EncryptionStrength
Archive created time
Zed! version used
Global IV
HMAC Key
IV for enc. HMAC
AES-CBC
User A (shared password)
Login: jdoe@domaine.fr
LoginMD5:
MD5
Privilege : ADMIN | Mandatory | ...
Salt (PBE)
Algorithm: SHA256
Loop Count (PBE)
Salt (PBA)
Loop Count (PBA)
Hashed Pwd:
Entry added on : YY-jul-2023 01:02.123456
AES-CBC
Archive Key
User 1
Login: jdoe@domaine.fr
RSA Public Key
LoginMD5, ...
Associated Zaf file: DOMAINE User1.zaf
Archive Key
Shared PWD A
ID 1
ID 2
Key
IV
RSA Public Key
RSA Private Key
RSA - PKCSv1.5 BT2

# C. ZONECENTRAL

# ZoneCentral

## Tour d'horizon

- Chiffrement de dossier, appelés « zones »
- Même éditeur, agrément DR
- Format des fichiers de zone `.zcctl` très similaire
- Chiffrement grâce aux `.zaf`

**Vulnérabilité 3**

Le HMAC des fichiers de zone peut être supprimé, silencieusement

**Remarque 3**

Chiffrement AES-CBC-ZED, IV = *filename*

```
XOR(petits fichiers avec même filename) = XOR(clairs)
```

# *ERRATUM*

## CE SLIDE NE FAIT PAS PARTIE DE LA PRESENTATION

**Remarque 3**

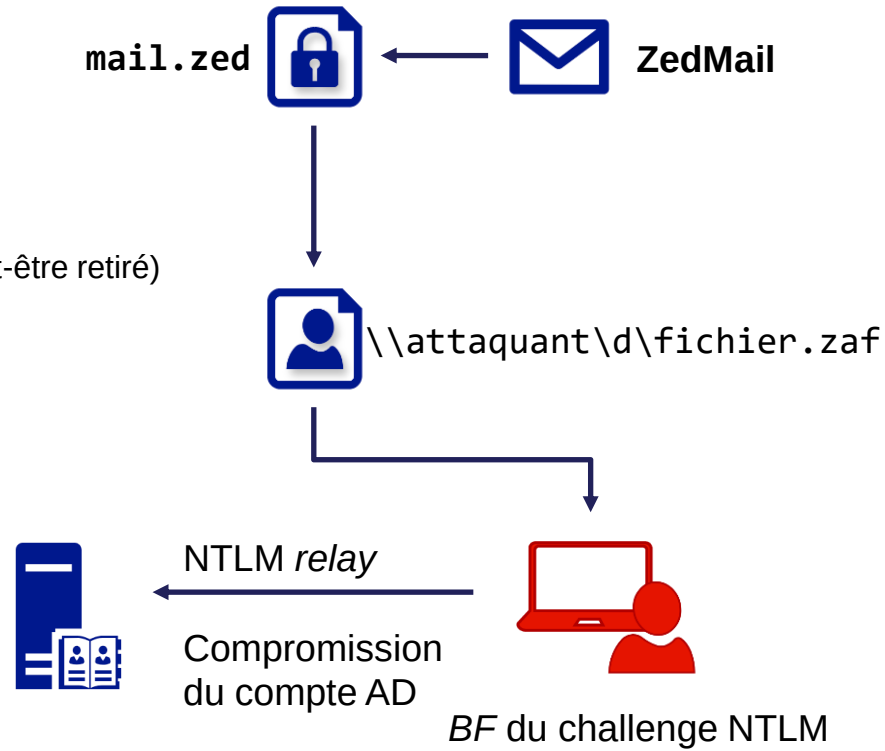
Chiffrement AES-CBC-ZED, ~~***IV = filename***~~

`XOR(petits fichiers ~~avec même filename~~) = XOR(clairs)`

L'IV ne dépend que de la Zone et du numéro du bloc (par bloc de 512octets)
Cette remarque est aussi valable pour le mode AES-CBC-CTS

# ZoneCentral + Zed!

- Chemin du fichier `.zaf` dans :
  - Le fichier de zone (donc modifiable, puisque le HMAC peut-être retiré)
  - L'archive (avant vérification de l'intégrité)




**Vulnérabilité 4**

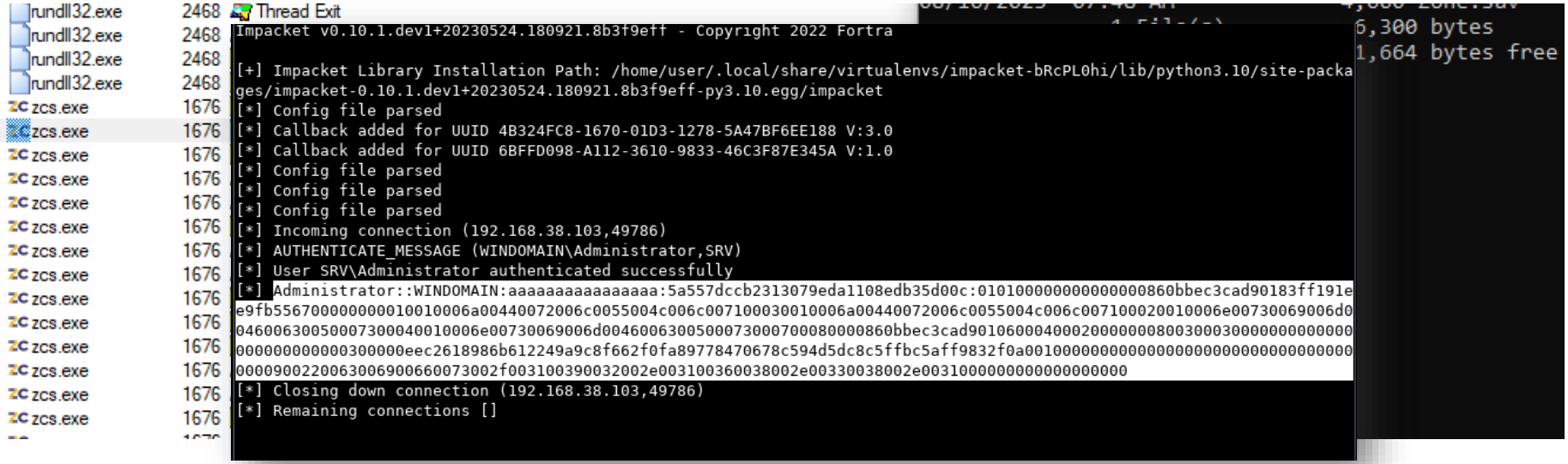
L'utilisation d'un chemin UNC provoque une authentification implicite

À l'ouverture d'un e-mail, d'une archive ou d'un fichier dans un répertoire partagé
→ Compromission possible du compte

# *Coerce* d'un utilisateur

Exemple : fichier de zone `.zcctl` malveillant (caché par l'explorateur)

Une écriture de fichier dans un sous-dossier déclenche la vulnérabilité



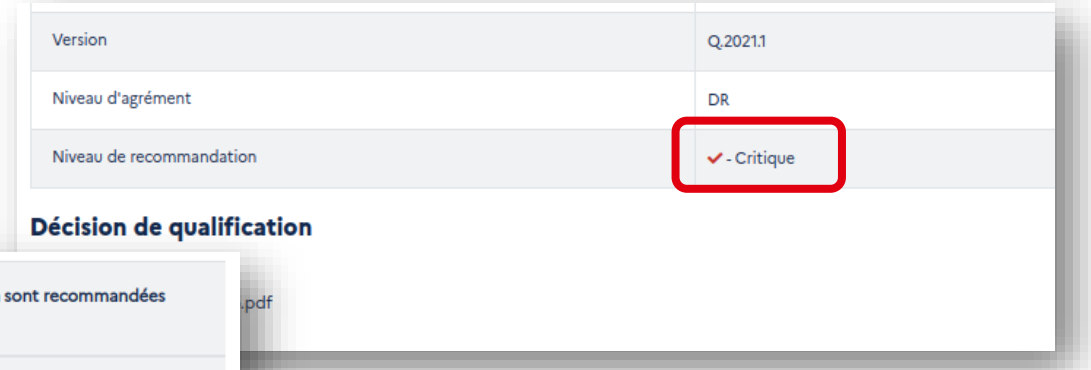
# 3. CORRECTIONS

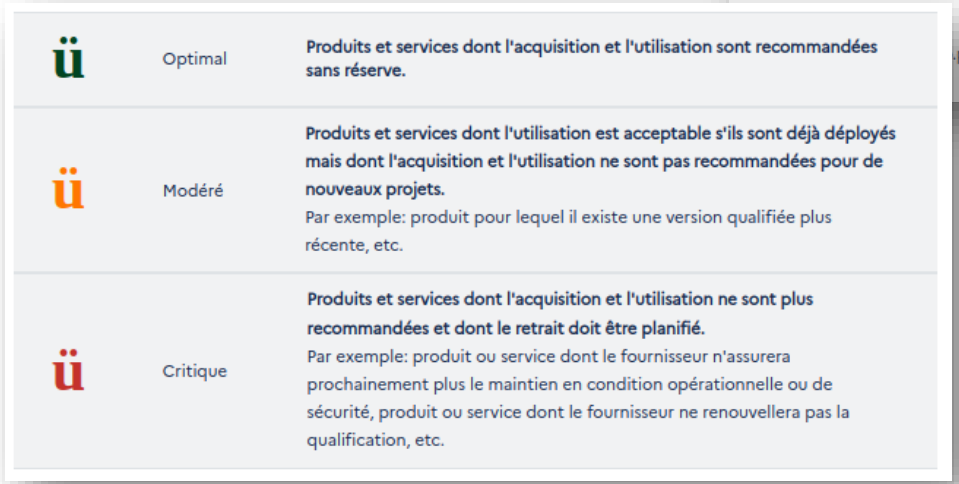
# Vulnérabilités et corrections

CVE-2023-5044 (8.7), CVE-2023-50439 (5.3), CVE-2023-50442 (4.1), CVE-2023-50442 (4.1), CVE-2023-50441 (4.8)
CVE-2023-50443 (4.0), CVE-2023-50440 (7.5)

- Corrections < 3 mois, avec des variants trouvés par l'éditeur
- Communication publique, perte de l'agrément et agrément de la nouvelle version
- Communications privée
  - Détails pour les bénéficiaires de l'agence
  - Détails pour les clients Prim'X

# Vulnérabilités




https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees

# Vulnérabilités

- Dans une version à jour, les archives ne contiennent plus :
  - Le `.zaf` du créateur
  - Le chemin de création
- Les chemins UNC ne sont plus pris en compte
- Que se passe-t-il si, temporairement, la solution qui a le monopole de fait n'est plus agréé pour le DR ?

Une analyse des données *leakées* (chemins, ZAF) doit être menée

Les fichiers ZAF doivent être entièrement renouvelés

# QUESTIONS

# MERCI POUR VOTRE ATTENTION !