

# Administration système

## Infrastructure

Un des fondateurs de l'association héberge une machine virtuelle contenant les services de l'association, entraînant une situation de sous-traitance. Un DPA a donc été signé entre l'association et son fondateur pour la gestion de cet hébergement.

L'hébergement consiste essentiellement à la mise-en-place de reverse-proxy (HTTP, DNS & SMTP) sur les services de l'association située dans une VM LXC.

DNS :

```
/etc/dnsmasq/dnsmasq.conf
newServer({address="10.0.0.2:53", pool="purr",
          checkName="purr-asso.eu.org.", checkType="SOA",
          healthCheckMode="lazy"})
addAction({'asso-purr.eu.org.'}, PoolAction("purr"))
```

SMTP :

```
/etc/smtpd.conf
action "purr" relay host smtp://10.0.0.2
match from any for domain "asso-purr.eu.org" action "purr"
```

HTTP :

```
/etc/nginx/sites-enabled/org.eu.asso-purr
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name asso-purr.eu.org *.asso-purr.eu.org;
    ssl_certificate /etc/ssl/private/org.eu.asso-purr.crt;
    ssl_certificate_key /etc/ssl/private/org.eu.asso-purr.pem;
    access_log off; # Traffic will already be logged on VM
    error_log off;
    root /var/www/html;
```

```

location / {
    proxy_pass https://10.0.0.2;
    proxy_ssl_verify on;
    proxy_ssl_trusted_certificate /usr/share/ca-
certificates/mozilla/ISRG_Root_X1.crt;
    proxy_ssl_name $host;
    proxy_ssl_server_name on;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto https;
    proxy_set_header Proxy "";
    proxy_pass_header Server;
    proxy_buffering off;
    proxy_redirect off;
    proxy_http_version 1.1;
}
}

```

À noter que dans le cas de HTTP, la clef privée de chiffrement des services a nécessairement du être recopiée sur la machine de virtualisation.

L'association met à disposition une url interne de PKI pour récupérer le certificat mis-à-jour via ACME :

```

/etc/nginx/sites-enabled/pki
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name pki;
    ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
    ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
    ssl_stapling off;
    access_log /var/log/nginx/pki.log;
    error_log /var/log/nginx/pki.log;
    root /etc/ssl/public;

    allow 10.0.0.1;
    deny all;
}

```

Les certificats sont de toute façon destinés à être publics, mais une solution plus idéale sera développée par la suite pour récupérer le certificat depuis l'URL public du site et procéder aux vérifications d'usage (non expiration, bon domaine, TLSA...) pour s'assurer qu'un certificat verroulé n'est pas déployé lors de son renouvellement.

# Hardening

## SSH

```
/etc/ssh/sshd_config/security.conf

Port xxx

PermitRootLogin prohibit-password
PubkeyAuthentication yes
PasswordAuthentication no
PermitEmptyPasswords no

Ciphers chacha20-poly1305@openssh.com
KexAlgorithms curve25519-sha256@libssh.org
MACs umac-128-etm@openssh.com

AllowUsers xxx yyy
```

## Nginx

```
/etc/nginx/conf.d/security.conf

server_tokens off;

ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers EECDH+CHACHA20:EECDH+AESGCM:EECDH+AES:!SHA;
ssl_prefer_server_ciphers on;
ssl_session_timeout 1d;
ssl_session_cache shared:SSL:50m;
ssl_session_tickets off;
ssl_stapling on; # Need because Let's Encrypt OCSP = Schrems II
```

```

ssl_stapling_verify on;
ssl_trusted_certificate /etc/ssl/certs/ca-certificates.crt;
resolver 127.0.0.1;

more_set_headers "Strict-Transport-Security: max-age=31536000; includeSubDomains; preload";
more_set_headers "X-Frame-Options: DENY";
#more_set_headers "X-XSS-Protection: 1; mode=block";
more_set_headers "X-Content-Type-Options: nosniff";
#more_set_headers "Content-Security-Policy: default-src 'none'";
more_set_headers "Referrer-Policy: same-origin";
more_set_headers "Expect-CT: max-age=86400, enforce, report-uri=\"https://aeris.report-uri.com/r/d/ct/enforce\"";
more_set_headers "Permissions-Policy: interest-cohort=()";

```

## Knot

```

1w      CAA      0 issue "letsencrypt.org"
;1w     CAA      0 issuewild ";"
1w      CAA      0 iodef "mailto:admin@purr-asso.eu.org"

```

## Liste de diffusion & mail

Les listes de diffusion de l'association sont hébergées par un [Schleuder](#) afin d'être intégralement chiffrées pour les seuls destinataires des listes de diffusion. Les clefs GPG associées sont diffusées [ici](#).

Dans le cas où un lanceur d'alerte ou autre personne sensible voudrait contacter l'association, il devrait d'abord récupérer cette clef et laisser dans les journaux son IP et la date de récupération de la clef GPG. L'association pourrait ultérieurement être perquisitionnée pour obtenir ces informations. La journalisation HTTP est donc désactivée pour cette URL :

```

/etc/nginx/sites-enabled/org.eu.asso-purr
location /.well-known/ {
    root /var/www/public/;
    access_log off;
}

```

Ces URL n'étant pas modifiable et ne servant pas de contenu à destination directe d'un utilisateur standard, cette modification ne met pas en défaut l'association de son obligation de conservation des journaux de trafic. L'association a procédé aussi à la vérification que la machine virtualisant ses services ne loggait pas non plus ces informations de consultation.

Les clefs ne seront pas publiées dans un annuaire de clefs, ceux-ci étant difficilement compatibles avec le RGPD (voir [ici](#) ([△ trackers google syndication](#)) et [là](#) ([△ trackers Medium](#))), l'association ne souhaite pas les mettre en avant d'autant plus qu'ils sont notoirement défectueux depuis plusieurs années.

Les clefs sont aussi disponibles via WKD.

```
gpg --auto-key-locate wkd --locate-key <xxx>@asso-purr.eu.org
```

Un script permet la synchronisation des clefs depuis Schleuder :

```
#!/usr/bin/env bash
set -e
schleuder-cli lists list | while read LIST; do
    FINGERPRINT="$(schleuder-cli lists show "$LIST" fingerprint)"
    echo "$LIST" "$FINGERPRINT"
    NAME="${LIST%*@}"
    DOMAIN="${LIST##*@}"
    KEY="$(schleuder-cli keys export "$LIST" "$FINGERPRINT")"
    WKD_DIR=hu
    ORIG="$DOMAIN/$NAME"
    echo "$KEY" | gpg --dearmor > "$LIST.asc"
    echo "$KEY" | gpg --show-keys --with-wkd-hash | \
        sed -En 's/^ +(\w{32})@.*\/\1/p' | \
        while read WKD_HASH; do
            ln -nfs "../$LIST.asc" "$WKD_DIR/$WKD_HASH"
        done
done
```

# Hébergement des mandats

L'association a vocation à collecter et à stocker des mandats de représentation afin de mutualiser des plaintes à la CNIL pour plusieurs personnes concernées. La signature d'un tel mandat nécessite la communication de pièces d'identité pour procéder à une vérification d'identité et éventuellement répondre aux demandes de responsables de traitement ou autorités de contrôle sans nécessité de reprendre contact avec la personne concernée. Les pièces d'identité étant des

données extrêmement sensibles, les données associées seront stockées sous 2 formats :

- en chiffrement end-to-end dans un redis temporaire, pour permettre aux modérateurs de vérifier la conformité du mandat et la véracité des pièces d'identité transmises. Ces données seront détruites à l'issue de la vérification, ce qui ne devrait pas dépasser quelques jours. De par le chiffrement e2e, seuls les modérateurs habilités pourront avoir accès aux données en clair. La consultation de ces documents ne pourra se faire que via une interface d'administration accessible après double authentification forte (authentification TLS cliente + TOTP).
- en chiffrement symétrique (chacha20-poly1305) via [Vault Transit](#), pour du stockage longue durée pour les besoins de gestion des plaintes et la réponse aux demandes des RT ou APD. La durée de rétention sera celle de la durée de traitement de la plainte associée.

## ## Vault

Le vault est scellé par [Shaamir](#), nécessitant l'intervention d'au moins 2 administrateurs pour relancer les services, ceci afin d'éviter toute vélocité de contrainte sur l'association.

Les premières tentatives de scellement du Vault ont échoué pour une raison inconnue et un message d'erreur cryptique. L'association aurait pu générer les secrets de Shaamir en clair et les chiffrer par la suite, mais il aurait alors existé une possibilité non nulle d'avoir un des administrateurs en possession de suffisamment d'information pour déverrouiller seul le Vault, ce qui aurait été contraire aux objectifs fixés initialement. Après debug, il s'avère que Vault attend obligatoirement des clefs GPG ayant les 2 flags `encrypt storage` et `encrypt communication`. Une des clefs des administrateurs désignés ne contenait que `encrypt storage` et pas `encrypt communication`, ce qui aurait du être pourtant suffisant pour Vault. La clef GPG en question a été modifiée et le scellement du Vault a pu être réalisé :

```
vault operator init -key-shares=3 -key-threshold=2 -pgp-keys=a.asc,b.asc,c.asc
```

# Administration système

- 24/01/2024 Un disque dur de la grappe RAID est HS. Retrait du disque + `shred -vz /dev/sdd` (triple passe + zeroed) avant retour fournisseur pour éviter accès aux données. Le disque est de toute façon chiffré intégralement.
- 31/01/2024 Mise-à-jour du serveur pour fixer CVE-2023-6246.

<https://security-tracker.debian.org/tracker/CVE-2023-6246> 2.36-9+deb12u4 fixed

```
# apt update && apt dist-upgrade
20:Réception de :3 http://security.debian.org/debian-security bookworm-security/main amd64
libc6-dev amd64 2.36-9+deb12u4 [1 897 kB]
```

```
25:Réception de :8 http://security.debian.org/debian-security bookworm-security/main amd64
libc6 amd64 2.36-9+deb12u4 [2 748 kB]
95:Préparation du dépaquetage de .../libc6-dev_2.36-9+deb12u4_amd64.deb ...
96:Dépaquetage de libc6-dev:amd64 (2.36-9+deb12u4) sur (2.36-9+deb12u1) ...
101:Préparation du dépaquetage de .../libc6_2.36-9+deb12u4_amd64.deb ...
105:Dépaquetage de libc6:amd64 (2.36-9+deb12u4) sur (2.36-9+deb12u1) ...
106:Paramétrage de libc6:amd64 (2.36-9+deb12u4) ...
275:Paramétrage de libc6-dev:amd64 (2.36-9+deb12u4) ...
```

L'hyperviseur a été aussi patché (confirmation du ST).

- 01/07/2024 : Mise-à-jour du serveur pour fixer CVE-2024-6387 (regeSSHion)

<https://security-tracker.debian.org/tracker/CVE-2024-6387> 1:9.2p1-2+deb12u3 fixed

```
# apt update && apt upgrade
36:Préparation du dépaquetage de .../01-openssh-sftp-server_1%3a9.2p1-2+deb12u3_amd64.deb ...
37:Dépaquetage de openssh-sftp-server (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
38:Préparation du dépaquetage de .../02-openssh-server_1%3a9.2p1-2+deb12u3_amd64.deb ...
39:Dépaquetage de openssh-server (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
40:Préparation du dépaquetage de .../03-openssh-client_1%3a9.2p1-2+deb12u3_amd64.deb ...
41:Dépaquetage de openssh-client (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
91:Paramétrage de openssh-client (1:9.2p1-2+deb12u3) ...
107:Paramétrage de openssh-sftp-server (1:9.2p1-2+deb12u3) ...
109:Paramétrage de openssh-server (1:9.2p1-2+deb12u3) ...
110:rescue-ssh.target is a disabled or a static unit not running, not starting it.
111:ssh.socket is a disabled or a static unit not running, not starting it.
```

L'hyperviseur a été aussi patché (confirmation du ST).

---

Revision #1

Created 15 August 2024 19:46:28 by aeris

Updated 15 August 2024 19:46:46 by aeris