Distribution EOLE - Tâche #35859

Scénario # 35830 (Nouveau): Le certificat Let's Encrypt ne sont pas reconnu à l'enregistrement_zephir

Etude

02/04/2024 12:57 - Emmanuel GARETTE

Statut:	Résolu	**Début:**	02/04/2024
Priorité:	Normal	**Echéance:**	
Assigné à:	Emmanuel GARETTE	**% réalisé:**	100%
Version cible:	Carnet Cadoles	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

analyse

Ubuntu fournit bien le fichier racine :

```
root@amon:~# openssl x509 -in /usr/share/ca-certificates/mozilla/ISRG_Root_X1.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            82:10:cf:b0:d2:40:e3:59:44:63:e0:bb:63:82:8b:00
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Validity
            Not Before: Jun  4 11:04:38 2015 GMT
            Not After : Jun  4 11:04:38 2035 GMT
        Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1
```

Par contre le Zéphir n'est pas signé via la racine, mais via le certificat R3 :

```
root@zephir:~# openssl x509 -in /etc/zephir/ssl/certs/zephir.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:50:93:37:ec:de:a2:7c:c4:82:a7:e9:ac:83:80:46:2f:13
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Feb  9 02:51:23 2024 GMT
            Not After : May  9 02:51:22 2024 GMT
```

Le certificat R3 est en fait un certificat intermédiaire :

```
root@zephir:~# openssl x509 -in /usr/local/share/ca-certificates/letsencryptauthorityr3.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Validity
            Not Before: Sep  4 00:00:00 2020 GMT
```

```
            Not After : Sep 15 16:00:00 2025 GMT
        Subject: C = US, O = Let's Encrypt, CN = R3
```

Ma solution proposée dans la demande parente fonctionne mais ce n'est pas une bonne solution.

Problèmes

- l'application Zéphir (tout comme Nginx, Apache, ...) ne fournit pas le certificat intermédiaire comme il devrait le faire
- EOLE ne devrait pas refournir les certificats racines et R3 de Let's encrypt, on devrait laisser Ubuntu et certbot pour le faire.

Comme on le voit en 2025 on va se retrouver avec un pb de certificat intermédiaire !

Solutions

- identifier les services utilisant LE (nginx, apache, twisted, ...)
- configurer les services pour diffuser le certificat intermédiaire LE
- supprimer la diffusion des certificats LE

Historique

#1 - 02/04/2024 12:57 - Emmanuel GARETTE

- Statut changé de Nouveau à Résolu

- Assigné à mis à Emmanuel GARETTE

- % réalisé changé de 0 à 100