NF16614 — GESTION AUTOMATIQUE DE CERTIFICATS AVEC LET'S ENCRYPT (LE)

Disponible depuis la version 8.04.0.35132

Voir la carte de la fonctionnalité : A classer

Gestion automatique des certificats avec **Let's Encrypt**.

Suite à une décision commune Mozilla et de Google dans l'objectif de sécuriser Internet, les certificats autosignés seront bientôt bannis de la toile. Afin que les services se basant sur une communication HTTPS puissent fonctionner (API, Interface de dialogue, PolarisPlus, ...), il est sera bientôt requis d'utiliser un certificat de sécurité valide au sens du W3C :

- valide dans le temps (non expiré)

l*imité dans le temps (max 2ans)

- reconnu par un tiers de confiance (Verisign, Symantec, Comodo, LE, ...)

Let's Encrypt est une initiative de l'IRSG avec de nombreux sponsors (EFF, Mozilla, Cisco, OVH...) visant à fournir des certificats SSL valides gratuits. Ces certificats étant valable 3 mois, il est nécessaire d'automatiser leur gestion.
Pour utiliser un certificat, il faut que ce dernier soit obligatoirement rattaché à un domaine, ce qui implique que :

- l'utilisation du dyndns interne (pl-vega-xxxx.vega-net.net) va devenir systématique : plus de connexion sur l'IP ;
- sécurisation des DNS utilisées de façon à ce qu'elles ne puissent pas être usurpées (DNSSec) ;
- sécurisation des adressages IP du DynDNS : il ne faut plus que chacun puisse se signaler comme étant le TLR (pour éviter une usurpation interne ou que toute la sécurité repose sur la possession de la licence) ;

Let's encrypt implique des rate limit, ce qui signifie que pour gérer tout le monde il va falloir plusieurs domaines donc -> abandon de vega-net.net pour le dyndns au profil d'un pool de domaine affecté par service (xxx.vs-api-1.net, yyyy.vs-api-2.net, ...) ;
Il nous faut un accès IP publique (pl-xxxx.vs-api-1.net)