

Se connecter

Proposer un contenu

Identifiant

Identifiant

Mot de passe

Mot de passe

☐ Connexion automatique

Se connecter

Pas de compte ? S'inscrire...

Journal : Projet qui viens de sortir

Posté par Richard DEMONGEOT (site web personnel) le 27 février 2026 à 18:10. Licence CC By-SA.

Étiquettes : pki, sspl



Hello,

Je viens de "finir" un projet de private key. Le but est d'avoir une PKI, qui réponds au protocole ACME, et qui permette de générer des configuration OpenVPN.

Le poc est fonctionnel, j'ai testé], ça semble fonctionner de mon côté.

Je dois valider encore quelques trucs, et le code sera publié.

Je dev sur ma forge (gitlab auto hébergé), on m'a conseillé de publier le code sur GitHub. Mais je peux changer de fusil d'épaule.

Je cherche maintenant à savoir - une fois que tout ça est fait :

- Est-ce que ce type de produit peut intéresser du monde?

La licence sera une SSPL, donc code ouvert, mais utilisation corporate soumise à licence (dans ma tête, un lien vers le site du projet, autorisation écrite d'afficher l'utilisateur comme "Ils nous utilisent").

Est-ce que certains d'entre vous veulent des comptes pour tester?

Cordialement,

(4 commentaires).

Markdown

E PUB

Infrastructure

Posté par Enzo Bricolo le 27 février 2026 à 18:51.

Évalué à 4 (+2/-0).

Dans PKI, le "I" c'est pour infrastructure.



"Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore public key infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels) ou matériel type Hardware Security Module (HSM ou boîte noire transactionnelle) ou encore des cartes à puces, de procédures humaines (vérifications, validation) et de logiciels (système et application) destiné à gérer les clés publiques des utilisateurs d'un système."

Tu peux nous décrire en 3 phrases ton infrastructure cible ?

Répondre

[^] # Re: Infrastructure

Posté par Richard DEMONGEOT (site web personnel) le 27 février 2026 à 19:13. Évalué à 2 (+2/-0).

Hello,



De manière très rapide, et actuellement :

Une interface/API disponible en web;
Un stockage MariaDB (clef chiffrées avec une option mdp utilisateur pour l'utilisiation).

Donc très méchamment, une interface WEB à un openssl + le repo GIT :).

Mais l'interface permet de valider / révoquer les certificats, de pousser un CSR (comme des scripts shell, on est d'accord) etc.

A moyen terme, utilisation de nitrokey en guise d'HSM hardware (ou intégration avec un autre HSM)

et autre vision souhaité faire du Shamir Shared Secret entre 3 membres de l'entreprise pour dévérouiller la clef ROOT.

Dès que j'ai assez avancé, le SSS pourrait être fait à partir de NitroKey utilisateur (donc 2 sur 3 utilisateurs pour reconstituer le mdp de la clef root, donc pour signer l'intermédiaire).

Et surtout, à moyen terme, possiblité de faire du Single Sign On avec le compte LDAP d'entreprise, donc le flux de création de compte VPN deviendrai :

- 1/ L'employé est créé dans l'IT en tant que salarié;
- 2/ il se logue sur l'interface, "je veux mon compte VPN"
- 3/ son certificat utilisateur est généré, ajouté au fichier ovpn, téléchargé par l'utilisateur;
- 4/ ça fonctionne.

L'idée est la même pour l'authentification des postes en wifi, ou pour toute authentification par certificat en entreprise.

L'autre avantage, la RH peut révoquer le certificat, la CRL se met à jour, et (si le VPN la lit ou la met a jour régulièrement), le compte VPN est coupé.

Répondre

SPSPL

Posté par Faya le 27 février 2026 à 21:12. Évalué à 2 (+0/-0). Dernière modification le 27 février 2026 à 21:12.

VU qu'il en faut toujours un, je me dévoue : la SSPL Sa Pue, Sai Pas Libre.

Histoire d'agréments le commentaire, pourquoi cette licence et pas une licence libre ?

Répondre

[^] # Re: SPSPL

Posté par Bruno (Mastodon) le 27 février 2026 à 21:28. Évalué à 1 (+0/-0).

Pour financer le projet avec ceux qui ont les moyens ?

C'est pas libre effectivement.

Répondre

Envoyer un commentaire

Suivre le flux des commentaires

Note : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

Derniers commentaires

- Re: ensemble
- Re: ensemble
- Re: SPSPL
- Re: ensemble
- Re: Everything in its ...
- SPSPL
- Dressé par une moule
- Re: Transfert entre p...
- Re: C'est pas Israël...
- Re: remédiation
- Re: Traduction appr...
- Re: Bientôt intedit

Étiquettes (tags) populaires

- intelligence_artificielle
- grands_modèles_de...
- merdification
- administration_fran...
- bronsonisation
- logiciel_de_caisse
- capitalisme_de_surv...
- états-unis
- politique
- microsoft
- jacques_ellul
- python

Sites amis

- April
- Agenda du Libre
- Framasoft
- Éditions D-BookeR
- Éditions Eyrolles
- Éditions Diamond
- Éditions ENI
- La Quadrature du Net
- Lea-Linux
- En Vente Libre
- Grafik Plus
- Open Source Initiative

À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr....
- Informations sur le s...
- Aide / Foire aux que...
- Suivi des suggestion...
- Wiki du site
- Règles de modération
- Statistiques
- API pour le développ...
- Code source du site
- Plan du site