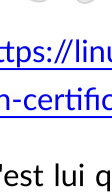


## Journal : Utiliser un certificat de signature électronique certinomis sur GNU/Linux Ubuntu (le retour...)

Posté par Paul POULAIN (site web personnel, Mastodon) le 25 avril 2024 à 17:39. Licence CC By-SA.  
Étiquettes : certinomis, signature, électronique, x509, clé, clé\_usb



Ce journal fait suite au fort intéressant journal de dark\_moule :

[https://linuxfr.org/users/dark\\_moule/journaux/utiliser-un-certificat-de-signature-electronique](https://linuxfr.org/users/dark_moule/journaux/utiliser-un-certificat-de-signature-electronique)

C'est lui qui m'a permis d'oser tenter d'acheter un certificat chez certinomis et l'installer sous mon xubuntu.

Je vous partage les écueils que j'ai croisés. La documentation fournie par certinomis est plus que minime, elle est indigente (autant que leur site web, qui date des années 1800, bref...)

### Installation initiale

Premier écueil : que faut-il installer ? Là, c'est tout simple, le paquet qui est ici : <https://www.certinomis.fr/drivers-gemalto> comme le dit dark\_moule.

Une fois que c'est installé, une petite applet apparaît :



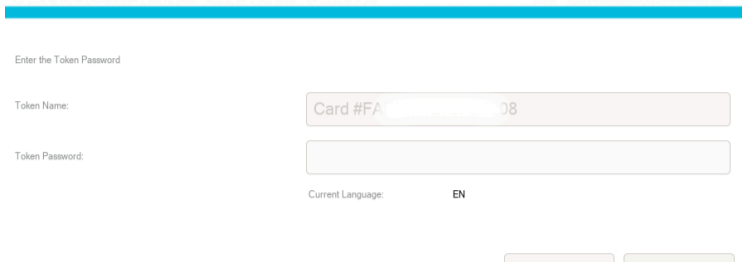
Le S est rouge lorsque la clé USB a été insérée.

Si en faisant clic droit > certificate information tu vois ton certificat (il y a 2 lignes, avec des numéros différents, je ne sais pas trop pourquoi), c'est que la 1ere étape est réussie :



Vérifions le code PIN : on sélectionne le certificat puis "Log On" en bas à gauche.

Saisissons le code PIN dans "Token password".



Si le code est erroné, message d'erreur. Si le code est bon, aucun message ni changement visible. Seule différence : on ne peut plus cliquer sur "Log On" (puisqu'on est loggué) (Ça m'a pas mal troublé)

Les autres options du menu de cette applet ne m'ont pas servi, en particulier le menu "unlock token" qui n'est PAS la saisie du code PIN

Maintenant que l'on a une clé opérationnelle, comment on fait pour signer...

### Thunderbird

C'est plutôt simple... jusqu'à THE écueil qui m'a tenu en haleine plusieurs heures. Je le mets en anglais (ça m'a beaucoup aidé de passer en anglais pour avoir des réponses de quant quand je buttais)

Thunderbird > Settings > Privacy and security > Security device > Load > new PKCS#11 module > Browse /usr/lib/libeTPkcs11.so

Apparaît alors :

▼ Nouveau module PKCS#11

Broadcom Corp 58200 [Contact...]

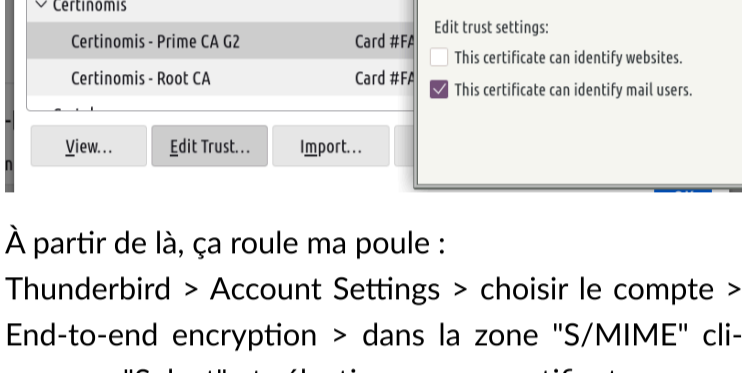
Broadcom Corp 58200 [Contactl...]

Feitian SCR301 (FFFFFFFFFFFFF...]

Et ensuite, je vous livre immédiatement LE truc qui a empêché que ça fonctionne pendant plusieurs heures. L'autorité certinomis n'était pas déclarée comme autorité de confiance pour signer des mails ! Pour l'activer, il suffit de :

Thunderbird > Settings > Privacy and security > Manage Certificates >

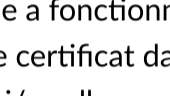
chercher certinomis dans la (longue) liste > cliquer sur "Certinomis Prime CA G2" puis sur "Edit Trust" :



À partir de là, ça roule ma poule :

Thunderbird > Account Settings > choisir le compte > End-to-end encryption > dans la zone "S/MIME" cliquer sur "Select" et sélectionner son certificat

Pour avoir le bouton qui permet de signer, personnaliser la barre d'outil de la rédaction d'un message (clic droit) et ajouter l'icône signature :



Je n'ai pas réussi à faire comprendre à libreoffice comment signer.

Par contre, pour Okular, ce qui est proposé dans le journal de dark\_moule a fonctionné :

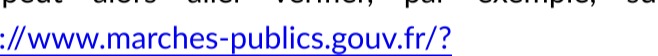
On crée le lien vers le certificat dans la base NSS  
mkdir -p \$HOME/.pki/nssdb  
certutil -N -d sql:\$HOME/.pki/nssdb  
modutil -dbdir sql:\$HOME/.pki/nssdb -add "OpenSC"  
-libfile /usr/lib/libeTPkcs11.so -mechanisms FRIENDLY

Okular > Configuration > Configurer les moteurs de rendu > PDF > saisir son code PIN (et, auparavant, le mdp qui aura été choisi lors de la commande certutil ci-dessus)

Pour signer un PDF, il suffit alors de l'ouvrir, puis Outils > Signature numérique en cours... > Tracer le carré de signature à la souris > sélectionner son certificat >

On obtient un joli :

La ville constate, après quelques jours de fonctionnement, des terlogiciel. Ce sujet sera à suivre dans le cadre de la maintenance.



On peut alors aller vérifier, par exemple, sur <https://www.marches-publics.gouv.fr/?page=Entreprise.VerifierSignature> que tout est OK :

Résultat du contrôle de signature du fichier

1 signature(s) détectée(s)

✓ Fichier signé. Signature valide

Et on peut enfin se détendre, fier du travail accompli (et, bientôt, signer des réponses à Appel d'Offre public !)

(10 commentaires).

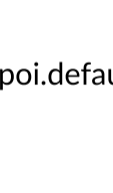
Markdown EPUB

### # LibreOffice > ça marche

Posté par Paul POULAIN (site web personnel, Mastodon) le 25 avril 2024 à 17:52. Évalué à 6.

Oh, si, en fait Libreoffice, ça marche.

Sauf que l'on ne trace pas la signature sur le document, donc on ne voit pas qu'il est signé.



Ce que j'ai fait pour le paramétrage :

LibreOffice > Tools > Security > Certificate Path >

Choisir thunderbird:default (et pas firefox) [le directory c'était

/home/paul/.thunderbird/499pzp0ierpoi.default

]

Ensuite, pour signer :

Fermer tout document libreoffice > File > digital signature > sign existing PDF (on ne peut pas signer un document ouvert en écriture)

Bon, au final, je préfère okular

### # Pas confiance

Posté par devnewton (site web personnel) le 25 avril 2024 à 22:08. Évalué à 7. Dernière modification le 25 avril 2024 à 22:08.

Il faut donc :

- insérer une clef USB (elle est sûre la clef? comment faire quand le RSSI a décidé du blocage de ces ports?) ;

- installer un pilote privateur

*Sans assistance ni support Certinomis.*



Comment avoir confiance en Certinomis dans ces conditions?

---

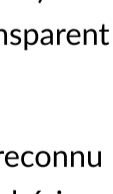
Le post ci-dessus est une grosse connerie, ne le lisez pas sérieusement.

#### [^] # Re: Pas confiance

Posté par Paul POULAIN (site web personnel, Mastodon) le 27 avril 2024 à 20:23. Évalué à 3.

yapa de RSSI qui décide de ce genre de chose dans ma PME, on est tous root sur nos machines,

Windows n'ayant pas droit de cité ;)



#### [^] # Re: Pas confiance

Posté par Olivier Serve (site web personnel) le 27 avril 2024 à 23:56. Évalué à 1.

Je ne connais pas le cas de Certinomis précisément, mais je doute qu'il s'agisse d'une clé USB, au sens de "périphérique mass-storage".



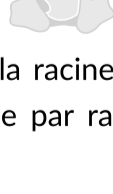
Il doit plutôt s'agir d'un lecteur de carte à puce avec une puce incluse (sans la carte autour). On en a au boulot, comme le plastique est transparent on voit la puce à l'intérieur.

Dans ce cas, le périphérique est reconnu comme lecteur de carte et non comme périphérique de stockage amovible. Et il n'est alors pas bloqué.

#### [^] # Re: Pas confiance

Posté par Paul POULAIN (site web personnel, Mastodon) le 29 avril 2024 à 09:53. Évalué à 2.

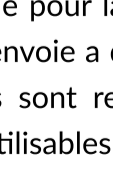
Je confirme que ce n'est pas une clé USB au sens de périphérique mass storage, mais un lecteur de carte à puce. Laquelle carte est d'ailleurs fournie à part du lecteur USB, c'est moi qui l'ai installé. Au renouvellement du certificat, il est possible de ne commander que la puce, et réutiliser le support USB



### # Intérêt du certificat

Posté par flan (site web personnel) le 26 avril 2024 à 12:59. Évalué à 6.

Pour moi, l'intérêt de payer pour un certificat réside dans le fait que son AC est connue des différents interlocuteurs. S'il faut ajouter une AC à la racine, est-ce que ça a vraiment une valeur ajoutée par rapport à faire sa propre AC ?



#### [^] # Re: Intérêt du certificat

Posté par dark\_moule le 26 avril 2024 à 23:15. Évalué à 4.

L'intérêt d'un tel certificat, pour l'usage que j'en ai, est dans le cadre professionnel. Il est ainsi possible d'établir des formalités auprès des greffes, de répondre aux appels d'offres, etc.



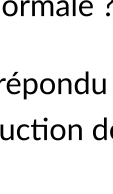
Je n'ai pas eu non plus de problème pour la signature de contrats ou de devis que j'envoie a d'autres entreprises. Les documents signés sont reconnus sans difficultés et sont facilement utilisables.

Sauf avec les banques où l'on m'a encore demandé d'envoyer un original papier pas plus tard que la semaine dernière, mais ça on ne pourra rien y changer.

#### [^] # Re: Intérêt du certificat

Posté par Paul POULAIN (site web personnel, Mastodon) le 27 avril 2024 à 20:18. Évalué à 6.

Comme l'a dit dark\_moule, pour signer des réponses à des AOs publics, c'est obligatoire. Il n'y a pas le choix, le certificat doit respecter certaines règles.



Évidemment, les auto-signés ne sont pas valables, et la clé USB est obligatoire. On peut le regretter, mais comme 99% de nos clients sont des structures publiques, yapa le choix. Jusqu'ici, on avait un poste sous windows juste pour ça, la clé sous Linux, c'est déjà un progrès ;)

#### [^] # Re: Intérêt du certificat

Posté par devnewton (site web personnel) le 29 avril 2024 à 14:18. Évalué à 3.

Quel est le cas d'usage où il y a tel doute sur l'identité de l'auteur de la réponse à un appel d'offre qu'un simple coup de fil ne suffirait pas à lever le doute sur une signature normale ?



- Allo, c'est vous qui avez répondu à l'appel d'offre pour la construction de l'autoroute A69 ?

- Oui, je suis Jean Michel Vinci.

- Votre signature ressemble à une bite ?
- Oui, c'est bien moi.
- Vous avez écrit à la page 42 que votre projet serait écoresponsable.
- Oui, on va même planter des arbres et préserver des ragondins protégés.
- Et vous livrerez dans les temps et conformes à vos engagements ?
- Oui comme sur tous nos chantiers.
- Monsieur, vos blagues ne font rire que vous.
- Arf grilled.

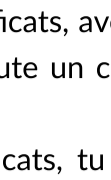
--

Le post ci-dessus est une grosse connerie, ne le lisez pas sérieusement.

### # Deux identifiants => deux certificats

Posté par Olivier Serve (site web personnel) le 28 avril 2024 à 00:01. Évalué à 3.

Si en faisant clic droit > certifi-  
cate information tu vois ton cer-  
tificate (il y a 2 lignes, avec des  
numéros différents, je ne sais pas trop pourquoi)



Tu as deux lignes car tu as deux certificats, avec deux numéros de série différents. Sans doute un certificat de signature et un de chiffrement.

Si tu as accès aux détails des certificats, tu devrais pouvoir le vérifier (chercher un champ "Key Usage").

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: Ça et autre chose
- Re: Hypothèses
- Re: Efface tout
- Re: Ça et autre chose
- Re: Efface tout
- Re: Efface tout
- Re: Efface tout
- Re: Hypothèses
- Re: Ça et autre chose
- Re: Ça et autre chose
- Re: Ça et autre chose
- Re: Efface tout

#### Étiquettes (tags) populaires

- intelligence\_artificielle
- merdification
- capitalisme
- grands\_modèles\_de...
- kokopelli
- linux
- états-unis
- bulle
- administration\_fran...
- sortie\_version
- donald\_trump
- vidéo

#### 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...
- Règles de modération
- Statistiques
- API pour le développ...
- Code source du site
- Plan du site