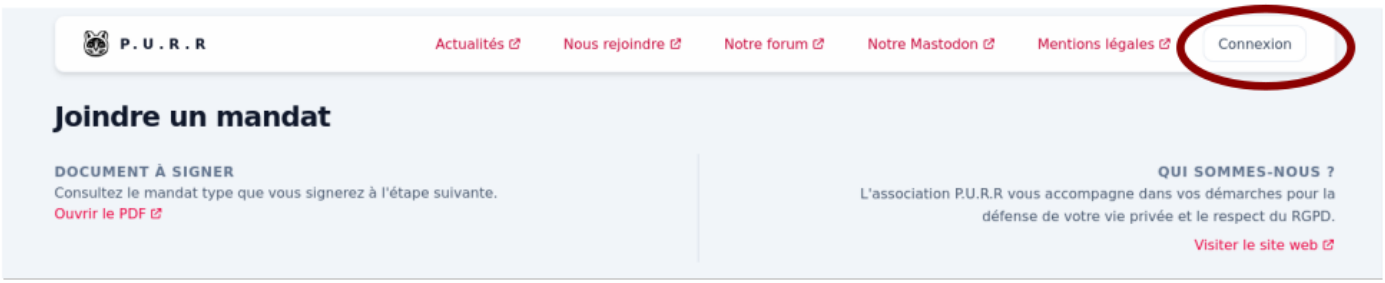
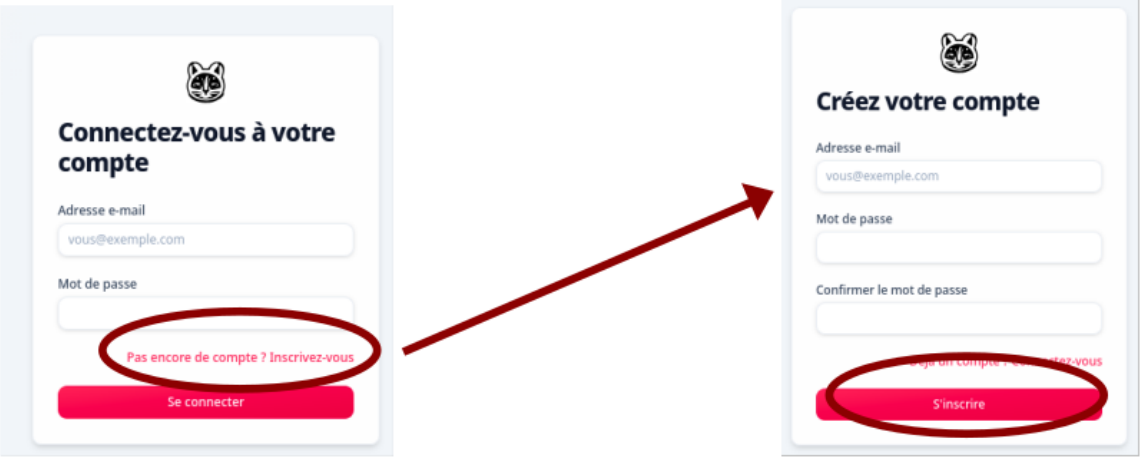
Accéder aux dossiers de plainte

1. Créer un compte

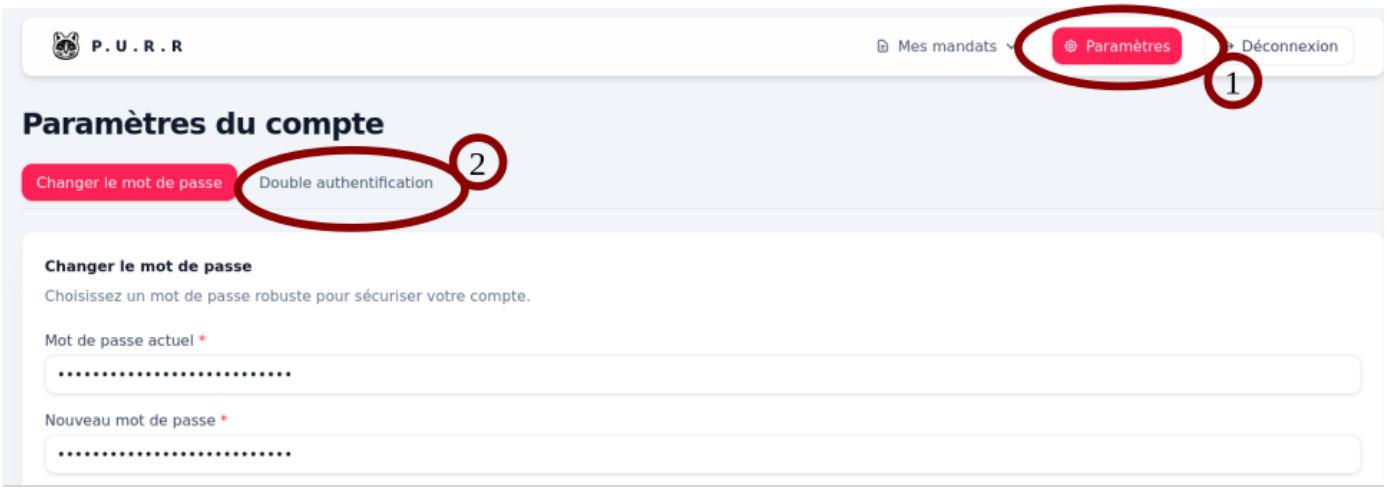
Aller sur https://agir.asso-purr.eu.org/

Aller dans connexion et suivre les étapes :





Lorsque vous avez créé votre compte, activez la double authentification en utilisant une application mobile telle que FreeOTP ou Aegis Authenticator.



Enregistrer de manière chiffrée les clés de secours.

Puis demander @aeris de passer admin, il va attribuer le pseudo que vous avez sur mattermost. (**Vérifier que c'est bien fait sinon en fin de course ça ne fonctionne pas**)

2. Obtenir un certificat pour pouvoir vous connecter au site

2.1 Sous Linux

Ouvrir un terminal dans le dossier dans lequel vous voulez enregistrer votre clé pour ça faire alt+maj+f4 dans le dossier ouvert ou clique droit et cherchez la ligne qui va bien

Remplacez `<pseudo>` par le pseudo que vous avez sur mattermost dans les prochaines commandes :

```
openssl req -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -subj "/CN=<pseudo>" -keyout <pseudo>.key -out <pseudo>.csr
```

Modifier, copier et coller la commande dans le terminal et l'exécuter.

Va apparaître : « Enter PEM pass phrase » il s'agit du mot de passe avec lequel sera protégée la clé privée. Il faudra donc s'en souvenir => enregistrement dans keepass par exemple.

puis

« Verifying - Enter PEM pass phrase » : retaper le mot de passe, pour confirmation.

Elle va afficher « ----- » (inutile de vérifier le nombre de tirets :D).

Elle va créer deux fichiers dans le dossier indiqué avant commande (si vous ouvrez votre terminal depuis votre librairie d'applications et que vous n'ajoutez rien ils seront dans votre home) :

- `<pseudo>.key` : il s'agit de la clé privée. Il ne faut jamais la donner à personne sous aucun prétexte.
- `<pseudo>.csr` : il s'agit de la demande pour rejoindre la pki.

Il faut la transmettre à Aeris (sur le mattermost ou en privé, peu importe, c'est un document public). Aeris va vous retourner votre certificat (-----BEGIN CERTIFICATE----- -----END CERTIFICATE-----).

TOUT copier-coller (y compris les lignes BEGIN et END) dans un éditeur de texte normal (pas un truc avancé comme writer, mais un truc normal comme gedit, pluma, nano, etc.).

Enregistrer ce fichier dans le même dossier que `<pseudo>.key`, et le nommer `<pseudo>.crt`.

Ouvrir un terminal dans le dossier où se trouvent tous les fichiers créés

La commande :

```
openssl pkcs12 -export -inkey <pseudo>.key -in <pseudo>.crt -name <pseudo> -out <pseudo>.pfx
```

Elle va demander : « Enter pass phrase for agir.asso-purr.eu.org.key: Enter Export Password: Verifying - Enter Export Password: »

Le premier, c'est le mot de passe de la clé privée, défini plus haut.

Les deux autres, le mot de passe qui protégera la clé privée dans la valise dont vous demandez la création. Il est recommandé de mettre le même puisque ça protège la même info.

Elle doit rien afficher de plus, et elle a créé un fichier agir.asso-purr.eu.org.pfx.

2.2 Sous Windows

A faire

2.3 Sous Mac

A faire

3. Ajouter votre certificat à votre navigateur

Aller dans les paramètre du navigateur (firefox ou dérivé)

Puis dans vie privée et sécurité

Puis descendre à "Sécurité" Puis dans "Certificat" sélectionner "Afficher les certificats". Une fenêtre "Gestionnare de certificats" va s'ouvrir rendez-vous dans l'onglet "Vos certificats" cliquez sur "importer" allez chercher le fichier `<pseudo>.pfx`.

Quand c’est fait une ligne est ajoutée, vous pouvez mettre ok et aller sur https://agir.priv.asso-purr.eu.org/login

Accepter l’utilisation du certificat

Rentrer login et mdp puis clé double authentification

Et normalement ça fonctionne ! sinon c'est que Aéris ne vous a pas passé admin :D

Revision #6
Created 2026-08-20 11:03:23 UTC by Mint
Updated 2026-08-20 11:37:13 UTC by aeris