Obtenir un certificat électronique personnel

Un certificat électronique personnel (aussi appelé certificat numérique personnel) vous permet d'authentifier vos communications ou de vous authentifier auprès d'un service tiers supportant l'authentification par certificats. L'université propose à tous les personnels, par l'intermediaire d'un prestataire de confiance, d'obtenir un certificat numérique personnel de manière autonome.

Un certificat électronique personnel n'est valide que pour un an et doit etre renouvellé tous les ans.

Procédure d'obtention

Le générateur de certificat électronique est disponible à l'adresse suivante:

https://cert-manager.com/customer/renater/idp/clientgeant

Authentification

Vous devez tout d'abord vous identifier sur le service en indiquant que vous faites partie de l'université puis en saisissant vos identifiants universitaires.

Vérification de vos informations

Le certificat électronique personnel devant vous authentifier, vous devez tout d'abord vérifier que le portail a bien récupéré les bonnes informations vous concernant:

Choix du type de certificat

Vous devez ensuite choisir le type de certificat que vous désirez:

- **GÉANT Personal Certificate** : C'est le certificat le plus courant, il vous servira à signer numériquement vos courriers électroniques. Vous pourrez aussi chiffrer vos emails avec celui-ci si votre version de Thunderbird le permet (version superieure ou égale à 78).
- **GÉANT IGTF-MICS Personal** : Ce type de certificat vous permettra de signer et de chiffrer vos courriers électronique mais aussi de vous authentifier auprès des services numériques nécessitant une authentification par certificat.

- **GÉANT IGTF-MICS-Robot Personal** : Ce type de certificat permet d'authentifier certains agent et processus logiciels devant se connecter sur une infra numérique sécurisée

Choix du type de clé

Votre clé privée doit être chiffrée pour garantir l'authenticité de la signature. Il existe plusieurs type d'algorithme de chiffrement. Vous pouvez aussi choisir de générer une requête de certificat.

Generate RSA : il s'agit de l'algorithme le plus courant et le mieux supporté **Generate ECC** : ECC est l'algorithme le plus récent et le plus sur. Il est supporté par Thunderbird, entre autre. **Upload CSR** : Si vous maitrisez la génération d'une requete de certificat, vous pouvez l'ajouter ici.

Choix d'un mot de passe

Votre clé privée va être chiffrée par un mot de passe qui vous sera demandée à l'ouverture du fichier de clé qui va être généré. **Vous devez conserver ce mot de passe précieusement**:

Téléchargement du fichier

Une fois les informations saisies et vérifiée, vous pouvez valider le formulaire. Vous devez ensuite accepter le contrat utilisateur du préstataire:

Vous obtenez ainsi un fichier de clé au format PKCS#12 (extension .p12) qui est accepté par la majorité des logiciels utilisant des certificats personnels.