

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'intermédiaire d'un prestataire de confiance, d'obtenir un certificat numérique personnel de manière autonome.

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 profil de certificat

Pour un certificat personnel qui sera utilisé dans la signature électronique, vous devez sélectionner GEANT Personal email signing and encryption.



Choix de la durée de vie du certificat

Vous êtes alors invité à choisir la durée pendant laquelle le certificat restera valide. A l'issue de cette période, il vous faudra générer un nouveau certificat.



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. Les clés RSA sont les plus courantes et plus leur taille est élevée plus ils sont surs. Les clés EC utilise un algorithme plus récent et plus sur. Ces 2 algorithmes sont supportés par Thunderbird. Vous pouvez aussi choisir d'utiliser une requête de certificat (CSR).



Choix d'un mot de passe

Votre clé privée va être chiffrée par un mot de passe qui vous sera demandé à chaque utilisation de votre clé (par exemple à chaque signature de document). **Vous devez conserver ce mot de passe précieusement**, sa perte nécessitera de générer un nouveau certificat:



Choix de la clé de l'algorithme de protection



Téléchargement du fichier

Une fois les informations saisies et vérifiées, vous devez ensuite accepter le contrat utilisateur du prestataire, puis valider le formulaire (Submit):



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.

From:
<https://wiki.univ-nantes.fr/> - Wiki

Permanent link:
https://wiki.univ-nantes.fr/doku.php?id=personnels:securite:certificats_personnels&rev=1697184437

Last update: 2023/10/13 10:07

