INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

Guide Utilisateur pour la mise en place d'un 2ème facteur d'authentification

à l'INSA Rennes

Table des matières

1. Principes de base

1.1. Qu'est-ce que la double authentification et pourquoi l'activer

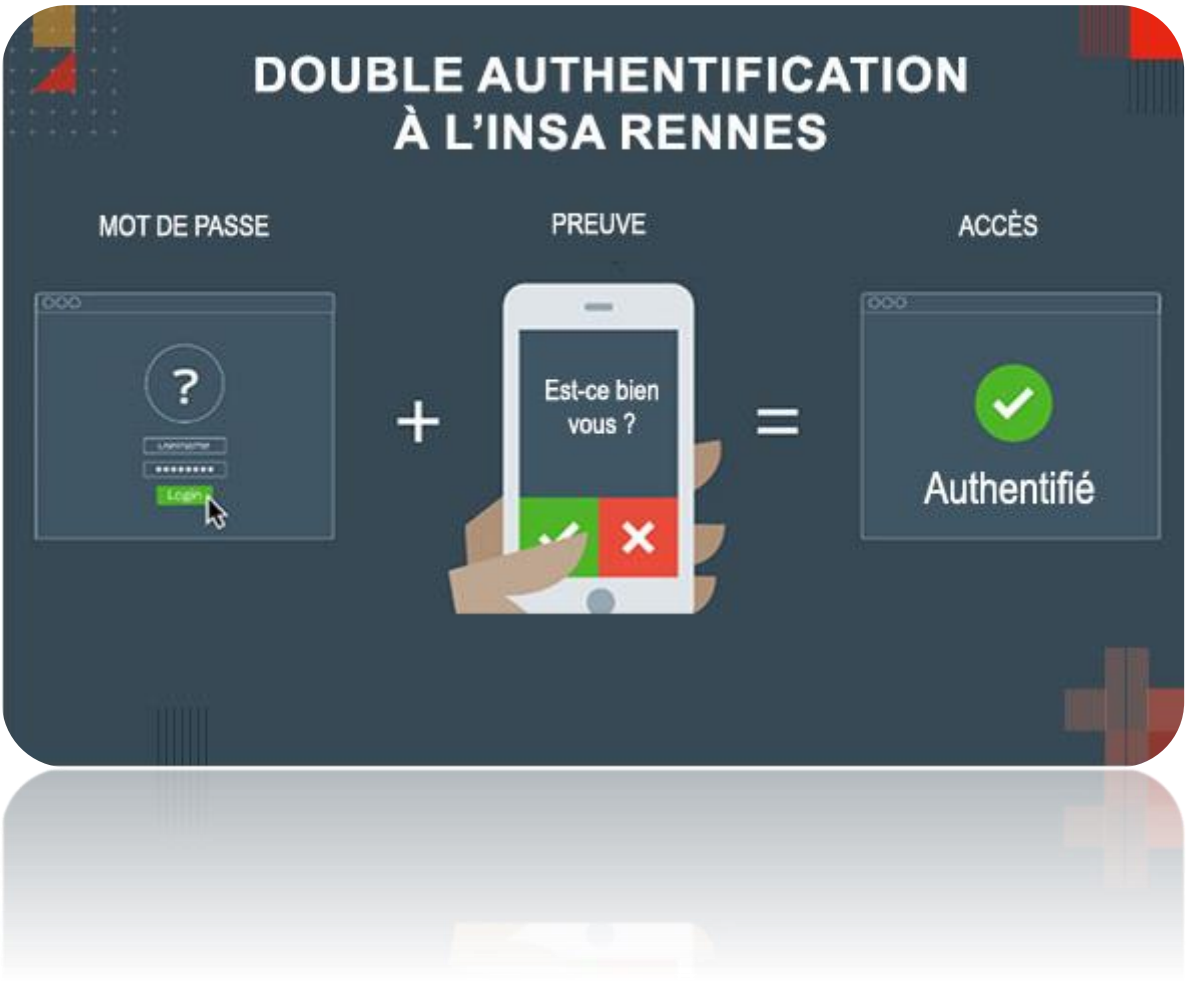
Vos identifiants sont essentiels pour vous connecter aux différents services de l'INSA comme la messagerie, l'espace numérique de travail (ENT) ou encore des applications métier distribuées. Pourtant, ils ne sont pas infaillibles et les cybercriminels n'ont aucune limite pour tenter de les pirater.

Pour faire face à une récente recrudescence des piratages de comptes informatiques à l'INSA Rennes, la DSI met en place la double authentification

La double authentification est une méthode d'authentification forte qui exige de l'utilisateur qu'il fournisse 1 facteur supplémentaire de vérification pour prouver son identité.

Le principe repose en grande partie sur l'envoi d'un code TOTP à usage unique, mais il existe d'autres possibilités comme l'envoi d'un mail avec un code, ou d'une notification push sur un téléphone mobile….

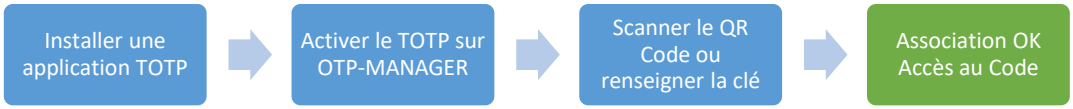
A l'INSA Rennes



1.2. Qu’est-ce que TOTP

TOTP signifie Time-based One-Time Password. C’est un code aléatoire de 6 chiffres, généré toutes les 30 secondes.

Il existe de nombreuses application TOTP mais le principe du TOTP est toujours le même :



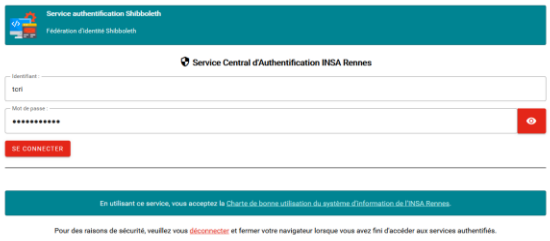
Activer la méthode Code temporel (TOTP) génère un QR Code et une clé

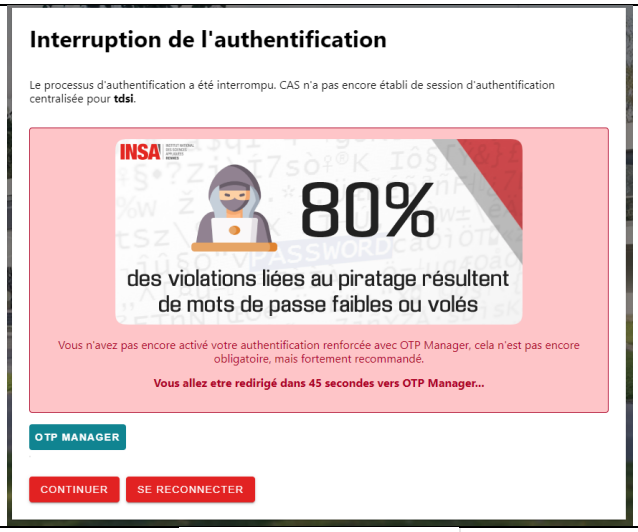
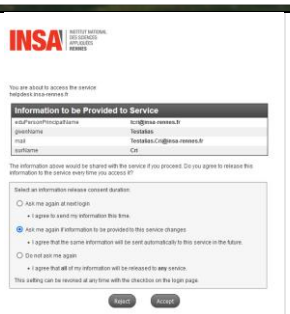
2. Avertissements

2.1. Période de transition

Le principe de double authentification deviendra, progressivement obligatoire pour l'ensemble de l'INSA Rennes et se généralisera à tous les services. La période facultative est de 1 mois.

Lorsque vous n'avez pas encore activé la double authentification

<table>
<tr>
<td>Authentifiez-vous avec vos identifiants INSA comme habituellement au service via le service central d'authentification</td>
<td> 
</td>
</tr>
<tr>
<td>Pendant la période non obligatoire vous verrez apparaître ce message avec le choix de continuer sans configurer

Configurer votre double authentification en cliquant sur OTP MANAGER
(cf. chapitre activation)</td>
<td> 
</td>
</tr>
<tr>
<td>Accepter pour confirmer les informations du fournisseur de service si nécessaire</td>
<td> 
</td>
</tr>
</table>

2.2. Double authentification obligatoire

Lorsque la double authentification sera obligatoire, vous n'aurez plus la possibilité de continuer vers votre service sans au préalable l'avoir configuré.

3. Recommandations

Le service de double authentification est rendu au travers de l'application Esup OTP disponible à l'adresse :

https://otp-manager.insa-rennes.fr/

Vous pouvez activer 3 facteurs d'authentification :

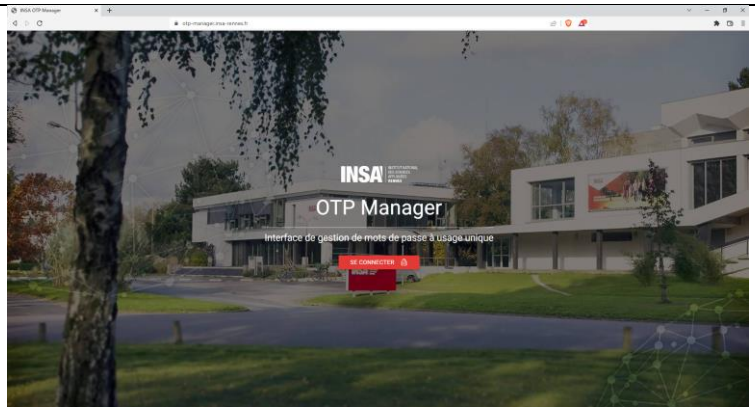
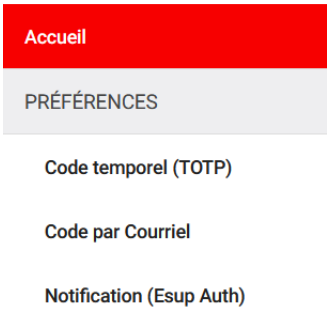
- Via une application TOTP (application pc ou smartphone)
- Via un envoi de code par mail (mail personnel)
- Par un push sur votre smartphone (application Esup Auth)

⚠	**La DSI vous recommande d'utiliser à minima 2 facteurs** L'installation d'une application mobile (TOTP ou PUSH) et la configuration par mail

4. Mise en œuvre de la double authentification

4.1. Procédures d'activation

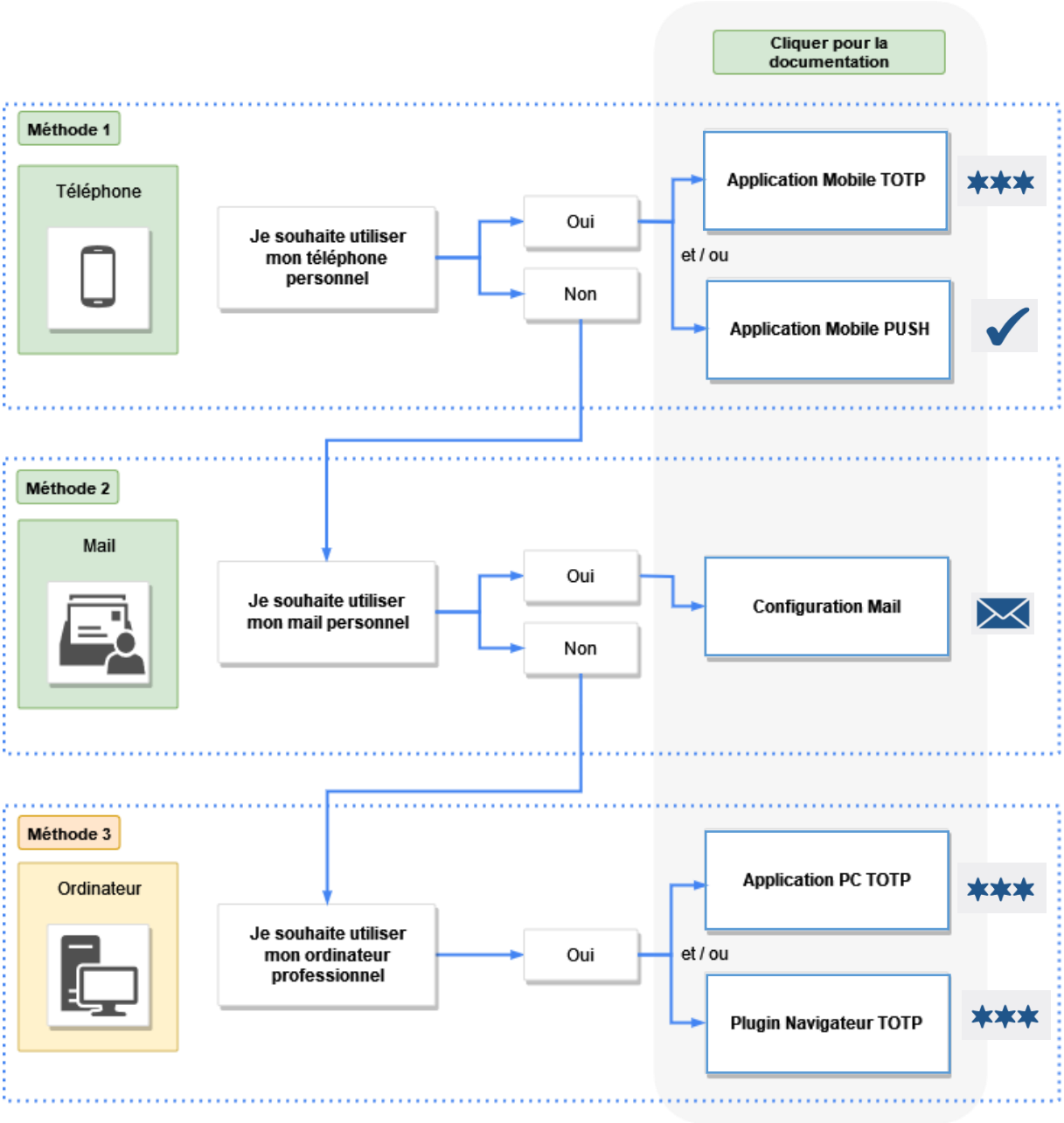
La 1ère étape consiste à activer une méthode d'authentification via l'application web ESUP OTP.

Connectez-vous à https://otp-manager.insa-rennes.fr/ Cliquez sur **SE CONNECTER**	
Cliquez sur le menu « préférences »	
Vous verrez les 3 possibilités d'activation dans le menu « Préférences »	
Recommandations	**Nous vous recommandons d'activer le Code Temporel (TOTP) sur votre téléphone portable personnel ainsi que l'envoi de code par mail personnel.** Cette configuration est la plus souple et couvre le + de cas d'usage notamment en cas de mobilité. Si vous n'activez que le mail, ou que le code temporel (TOTP) avec le plugin navigateur ou l'application sur ordinateur, vous pourriez vous retrouver bloqué si vous demandez un service numérique en dehors de l'INSA sans votre matériel enrôlé.
Avertissement	La solution ESUP OTP ne permet pas de réafficher le QR Code et la clé après avoir quitté le menu/la fenêtre. A l'instant, nous n'avons pas de solutions à vous proposer hormis de faire une capture d'écran ou noter la clé dans un coffre-fort

4.2. Cas d'usages

Vous trouverez ci-dessous les différentes méthodologies par ordre de recommandations ainsi que les liens directs vers les documentations associés.

Cette illustration est cliquable pour renvoyer vers les bonnes sections du document

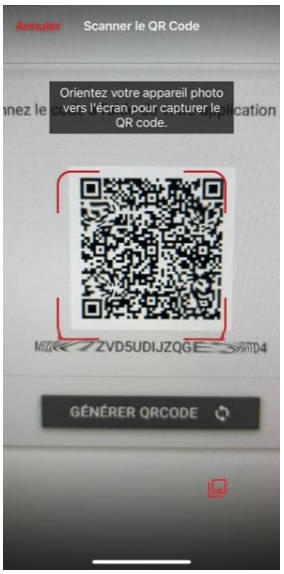


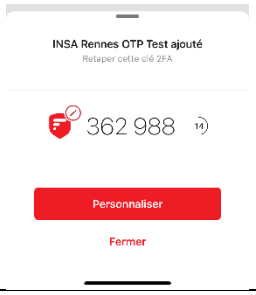
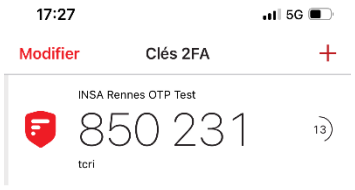
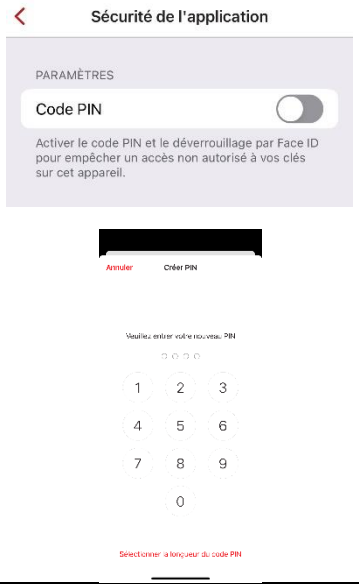
5. Les outils proposés

5.1. Application TOTP sur téléphone portable

Configuration de l'application mobile « 2FA Authenticator » disponible sur IOS et Android

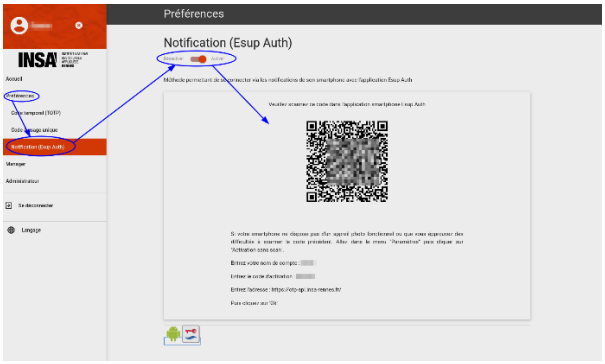
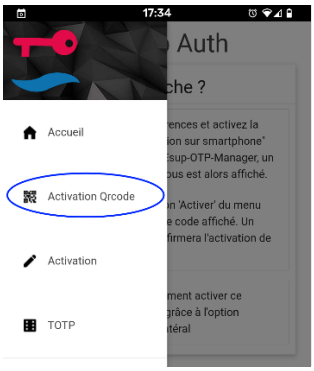
Il existe bien entendu d'autres applications sur téléphone portable comme Google Authenticator, Microsoft Authenticator, mais la DSI recommande cette application car elle est simple, clair visuellement, open source…

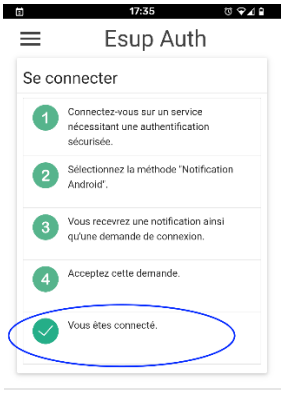
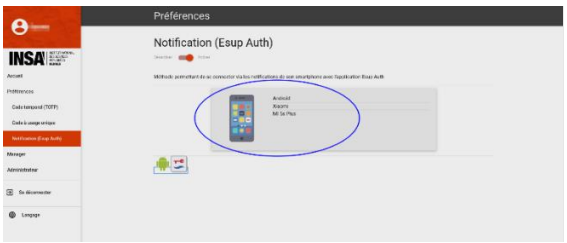
Installé classiquement l'application à partir de votre store habituel Une fois l'application installée à partir de votre store sur votre téléphone et lancée, cliquez sur le + pour ajouter un nouveau compte Puis Cliquer sur « Associer un nouveau service »	
Choisissez ensuite « Scanner le QR Code » qui est sur l'application OTP-Manager	
Scannez le QR sur votre écran d'ordinateur (cf. chapitre activation) avec la caméra de votre téléphone portable	

Une fois le QR Code scanné, le Compte est associé et ajouté	
Une fois l'application associée, vous verrez le nom du service et votre login Ainsi que le code TOTP à 6 chiffres avec une indication de la durée de validité en cours (sur 30 secondes)	
Vous avez la possibilité de protéger l'accès à l'application en activant un code pin Pour ce faire allez dans « Paramètres » Puis dans « Sécurité de l'application »	
Activer ensuite le Code PIN et créez en 1 pour l'accès à cette application	

5.2. Notification push avec Esup Auth (application Android et IOS)

Après avoir installé l'application « Esup Auth » sur votre mobile, vous pouvez configurer le mode push comme ci-dessous.

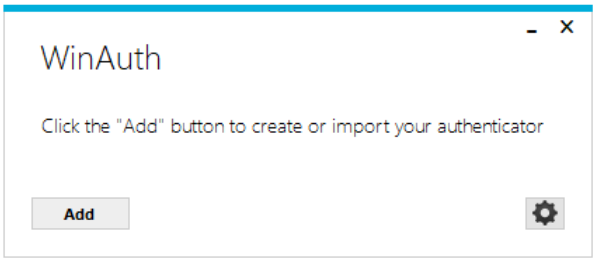
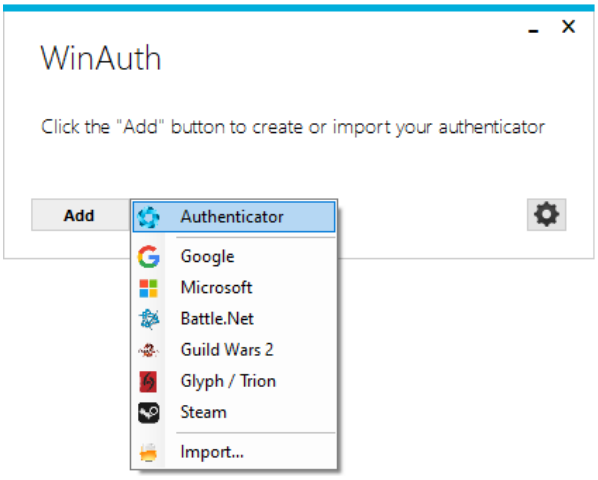
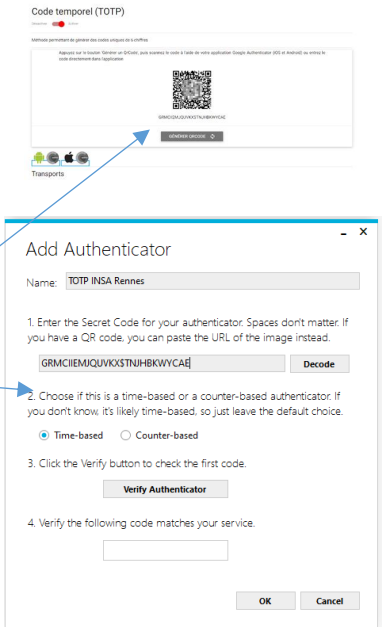
En activant la méthode Notification (Esup Auth), vous aurez accès à un QR Code et une clé alphanumérique	
Sur votre téléphone Android, installez l'application Esup Auth Puis via le menu en haut à gauche	
Cliquez sur « Activation QR code »	

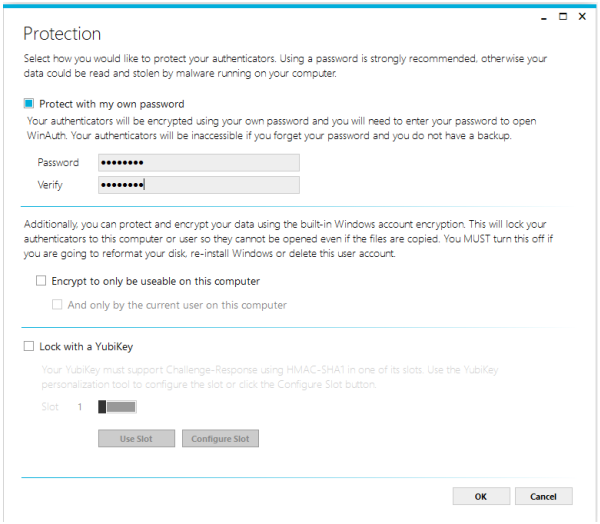
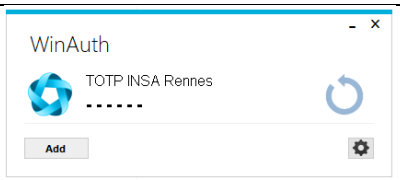
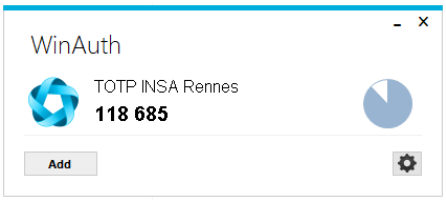
Scannez le QR sur votre écran d'ordinateur avec la caméra de votre téléphone portable	
Une fois le code scanné, l'application vous confirmera la bonne association de votre téléphone	
Une fois le processus terminé, vous verrez votre matériel (type de téléphone…) dans OTP Manager	

5.3. Application TOTP sur un ordinateur

Configuration de l'application WinAuth Windows présente sur les machines de l'INSA Rennes.

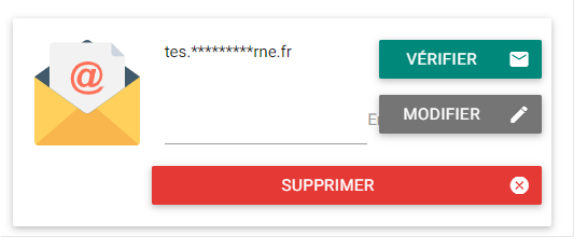
NB : Pour les postes non gérés par la DSI, l'application est également téléchargeable à l'adresse suivante : https://winauth.github.io/winauth/download.html

Au lancement de l'application on vous demande de renseigner les informations correspondant à votre code TOTP précédemment activé. Pour cela cliquez sur le bouton **Add**	
Sélectionnez **Authenticator**	
Donner un nom à votre configuration ex : « TOTP INSA Rennes » Entrer le code généré à l'étape précédente (n'accepte pas le copié collé), Chapitre activation Ok pour valider Puis Ok pour afficher la fenêtre suivante	

Une fenêtre s'ouvre vous proposant de sécuriser votre fichier de configuration avec un mot de passe *. Un fichier xml est ainsi construit et est situé par défaut dans votre %Appdata% : **C:\Users\%username%\AppData\Roaming\WinAuth** Lorsque vous êtes connecté dans une salle de TP, celui-ci-sera généré dans votre %homedrive% : **H:\Winauth**	
Une fois la configuration effectuée, cliquez sur le bouton d'actualisation pour visualiser votre code. * L'utilisation d'un mot de passe différent de celui de votre compte INSA est fortement conseillé. Vous devrez le renseigner à chaque démarrage de l'application	 

	Si vous souhaitez exporter cette configuration sur un autre support (clé USB, drive …), il suffit de sauvegarder les fichier WinAuth.exe et winauth.xml et de les placer dans le même répertoire. A l'exécution l'application prendra en compte les informations du fichier winauth.xml situé au même emplacement.

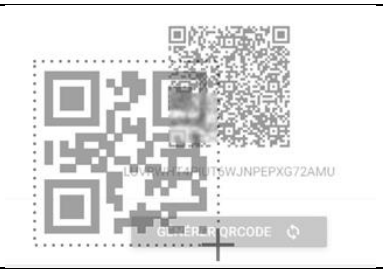
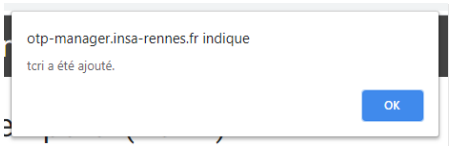
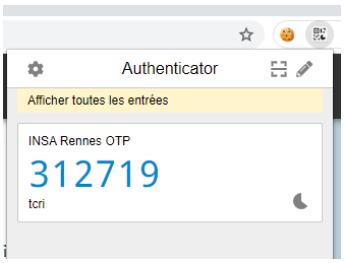
5.4. Mail : Code par courriel

Dans l'application Esup OTP : https://otp-manager.insa-rennes.fr Activez le code par courriel Sélectionnez « Code par Courriel » dans le menu « Préférences » Enfin cliquez sur **Activer**	
Une fois activé, vous devrez renseigner votre adresse mail personnelle (externe à l'INSA) Vous ne devez pas utiliser l'adresse mail INSA car le webmail INSA fait aussi partie des services nécessitant la double authentification.	
Si vous retournez ensuite sur ce menu, le mail n'est pas visible dans son intégralité et vous pouvez tester le bon fonctionnement en cliquant sur le bouton « Vérifier »	
Exemple du mail de test reçu	

5.5. Plugin TOTP dans un navigateur web

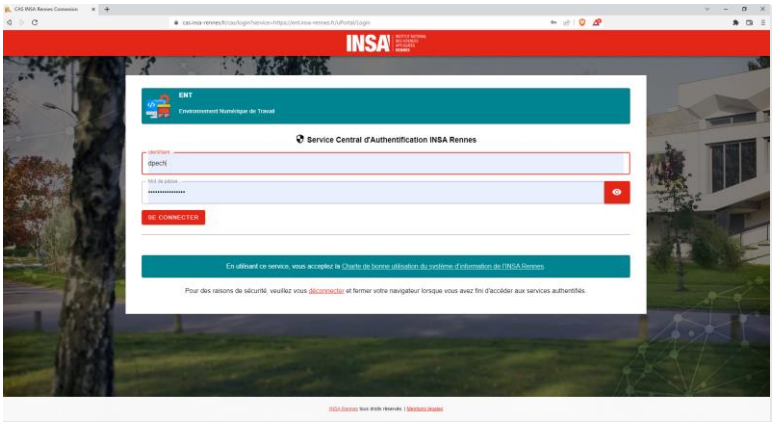
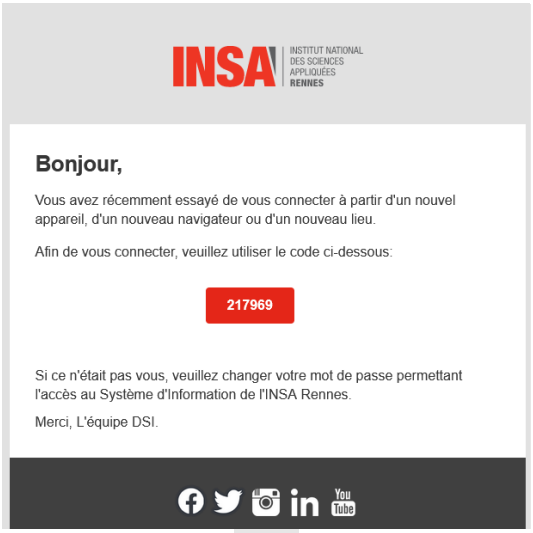
Configuration du plugin « Authenticator » pour chrome et firefox

- Lien Chrome : https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai?hl=fr
- Lien Firefox : https://addons.mozilla.org/fr/firefox/addon/auth-helper/

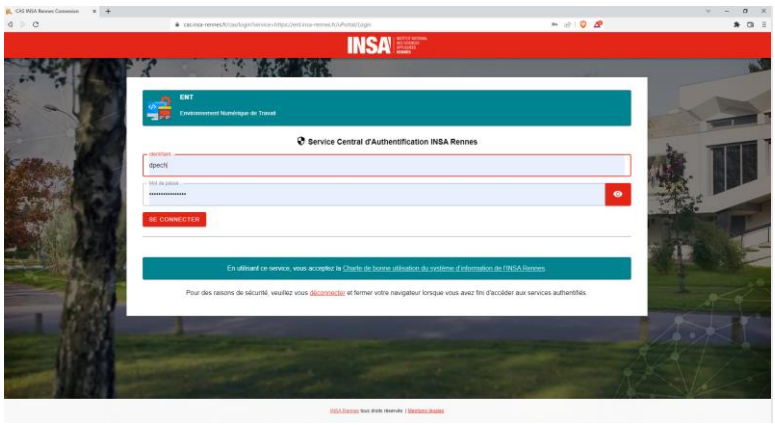
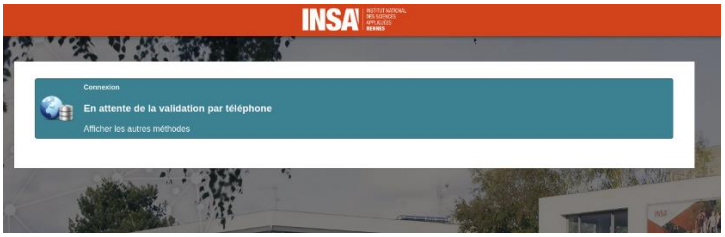
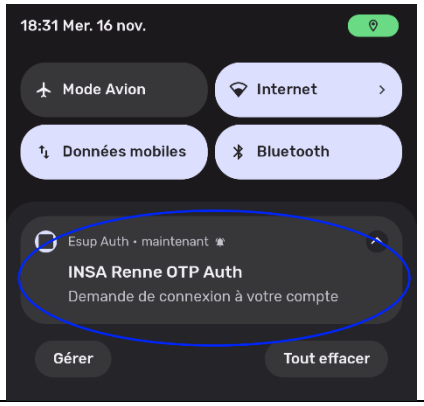
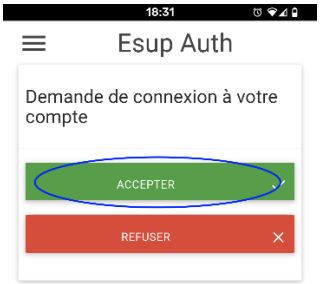
Une fois installée dans votre navigateur vous verrez l'icône dans la barre d'outils	
Il faut ouvrir la fenêtre sur otp-manager en affichant le QR code, et cliquer sur l'icône du plugin pour permettre de le « scanner » (cf. chapitre activation)	
Il suffit ensuite de faire de sélectionner avec la souris autour du QR code	
Un message indique que la configuration est réussie	
Vous avez désormais accès au code TOTP en cliquant sur l'icône du plugin	

6. Fonctionnement

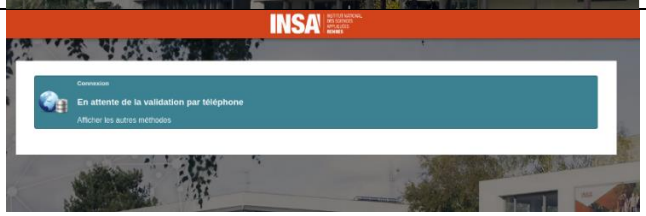
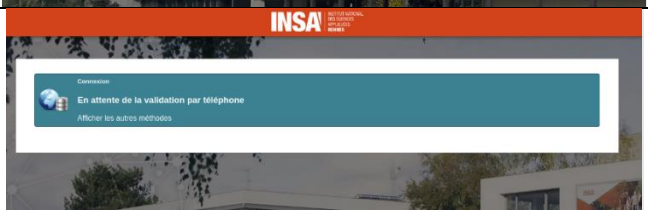
6.1. Fonctionnement du code à usage unique envoyé par mail

Connectez-vous à un service numérique web : https://ent.insa-rennes.fr et authentifiez-vous comme d'habitude sur le SSO-CAS avec vos identifiants INSA	
Une nouvelle fenêtre est proposée pour renseigner un code Cliquer sur le bouton mail pour envoyer le code sur l'adresse perso	
Vous recevrez un mail (charté INSA) avec un code sur 6 chiffres généré	

6.2. Fonctionnement avec Esup Auth

Connectez-vous à un service numérique web : https://ent.insa-rennes.fr et authentifiez-vous comme d'habitude sur le SSO-CAS avec vos identifiants/mot de passe INSA	
Une nouvelle fenêtre s'affiche indiquant l'attente de la validation par le téléphone (push)	
Vous recevrez donc une notification sur votre téléphone Cliquer sur la notification pour ouvrir directement l'application	 
Il suffit d'accepter la demande de connexion. Votre connexion à l'application continuera automatiquement après la validation.	

6.3. Résumé des différents affichages selon les méthodes choisies

Si choix unique de l'application TOTP	
Si choix unique du mail	
Si choix unique Esup Auth	
Si choix de l'application TOTP et mail	
Si mail + Esup Auth Esup Auth est prioritaire et il faut faire **"Afficher les autres méthodes"** pour afficher le reste	
Si application TOTP + mail + Esup Auth Esup Auth est prioritaire et il faut faire "Afficher les autres méthodes" pour afficher le reste