

Double authentification avec l'application Google Authenticator

L'application **Google Authenticator** permet de **générer des codes** avec un téléphone sans connexion internet ou service de téléphonie mobile. Ce code valide l'authentification en 2 étapes proposée par SIRÉM.

Cette manipulation consiste à sécuriser l'accès à son compte SIRÉM par une **double authentification** identifiant / mot de passe et validation par un **code reçu** sur l'application de son Smartphone (Apple, Android, Windows phone).

Télécharger l'application

Rendez-vous sur **Google Play**, l'**App Store** ou **Windows phone** afin de télécharger gratuitement l'application Google Authenticator :

- [Google Authenticator pour Android](#)
- [Google Authenticator pour Iphone](#)
- [Authenticator pour Windows phone](#)



Configurer l'application pour SIRÉM

Depuis la page de création de compte de SIRÉM ([page de création de compte](#)), le site vous propose un **QR code** (code-barres) à scanner depuis l'application Google Authenticator et une clé (*prenez à la noter, elle ne sera plus disponible après activation du compte, mais sera utile en cas de changement de téléphone ou paramétrage de WinAuth en plus de Authenticator*).

Paramétrer la validation en 2 étapes

Accès direct
Principaux
Autres orgs

Nom : *
Prénom : *
Date naissance : *

SIREM bénéficie d'une authentification à deux facteurs.
Un identifiant et un mot de passe que vous avez indiqué dans le formulaire ci-dessus et une clé secrète que vous devez inscrire dans un premier temps dans la zone 'Code de sécurité' ci-dessous qu'il faudra utiliser par la suite à chaque demande d'authentification.
Pour générer cette clé, vous devez utiliser un logiciel tiers qui devra être installé sur votre smartphone, tablette ou ordinateur de bureau.
Consultez le guide : [Installation du logiciel d'authentification](#)
Une fois installé, il faut référencer SIREM dans votre logiciel d'authentification. Vous devez créer un compte en ajoutant :

Manuellement	Automatiquement
Compte : @www.pprod-sirem.cnmosib.dirisi.defense.gouv.fr	En flashant le QR Code ci-dessous si vous utilisez un smartphone ou une tablette :
Clé : JV5E7YLNXLXUJZBJX	

Cette étape de référencement n'est à réaliser qu'une seule fois.
Code de sécurité : *

S'inscrire ou Annuler

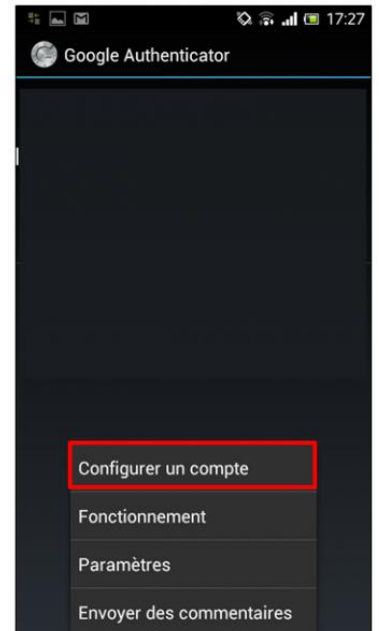
1

Depuis votre Smartphone, **ouvrez l'application Google Authenticator**.



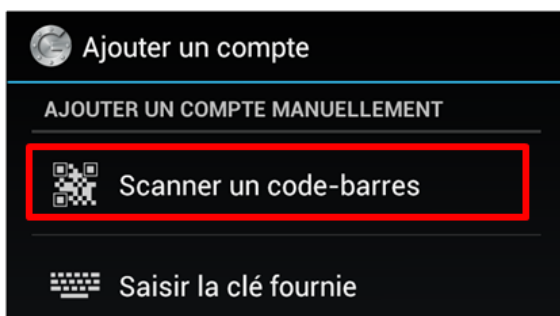
2 Démarrer l'application sur smartphone

La première utilisation de l'application nécessite l'**ajout du compte**. Appuyez sur l'icône **menu** puis sur **Configurer un compte**.



3 Configurer un compte

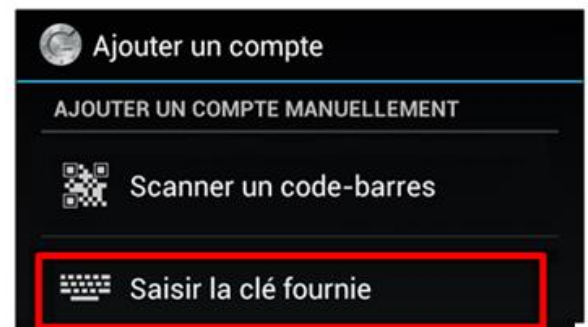
L'application vous invite ensuite à **scanner un code-barres**. Il s'agit du QR code affiché sur la page de création de compte SIRÉM de la validation en 2 étapes proposée sur votre ordinateur.



Association par scanner du code-barres

Dirigez **l'appareil photo** de votre Smartphone **sur le QR code** affiché sur la page de création de compte SIRÉM.

4



Association par clé

Utiliser la clé affichée affiché sur la page de création de compte SIRÉM.

5

Pour terminer l'association du téléphone avec votre ordinateur, un **code de validation** s'affiche sur votre smartphone. Vous devez le renseigner sur votre ordinateur sur la page de validation en 2 étapes et cliquez sur **Valider** (**Cette étape de référencement n'est à réaliser qu'une seule fois**).



Double authentification avec l'application WinAuth

L'application **WinAuth** permet de **générer des codes** sur un ordinateur. Ce code valide l'authentification en 2 étapes proposée par SIRÉM.

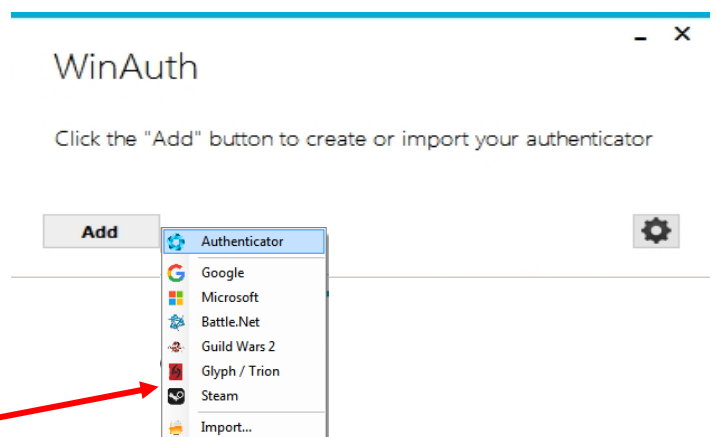
Cette manipulation consiste à sécuriser l'accès à son compte SIRÉM par une **double authentification** identifiant / mot de passe et validation par un **code reçu** sur l'application portable WinAuth, utilisable depuis une clé USB.

Télécharger l'application

Rendez-vous sur le site <http://winauth.com> et télécharger la version stable. Décompresser la, et placer le fichier « WinAuth.exe » sur une clé USB ou directement dans un dossier de votre choix sur votre ordinateur. Il s'agit d'une version portable qui ne nécessite pas d'installation.

1

Lancez l'application WinAuth.exe. *Si vous avez un message d'erreur qui vous informe de l'absence de Microsoft's .NET, vérifiez qu'il est bien installé. Si ce n'est pas le cas, installez ce produit et relancer WinAuth.*



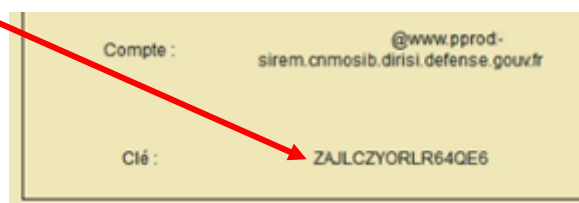
2

Cliquez sur le bouton 'Add' dans la liste des types d'authentification possibles, choisissez 'Authenticator'.

3

- Dans le champ '**Name**', remplacer « Authenticator » par le nom de votre choix. Exemple : 'SIRÉM PPROD'.

- Renseigner le champ 1 '**Enter the secret code for your authenticator**', avec la clef fournie par le site SIRÉM.



- L'option 2 '**Time based**' doit être cochée.

- Cliquer sur le bouton 3 '**Verify Authenticator**' pour vérifier si la clef saisie est valide. Si c'est le cas, vous verrez apparaître la première clef secrète.

4

Vous pouvez vérifier le bon fonctionnement en reportant cette clef dans la zone 'Clé secrète' ou 'Code de sécurité' de SIRÉM

4. Verify the following code matches your service.

560453


OK Cancel

Manuellement Automatiquement

Compte : @www.pprod-sirem.cnmosib.dirisi.defense.gouv.fr

Ciè : JV5E7YLNXLXJUZBJX

En flashant le QR Code ci-dessous si vous utilisez un smartphone ou une tablette :



Cette étape de référencement n'est à réaliser qu'une seule fois.

Code de sécurité

S'inscrire ou Annuler

5

Cliquez sur le bouton 'OK' de WinAuth pour sauvegarder la configuration que vous venez de réaliser. **NE SAUTEZ PAS CETTE ETAPE.**

6

WinAuth vous proposera de protéger l'accès à vos comptes. Pour cela, vous pouvez entrer un mot de passe et sa confirmation. Un clic sur le bouton 'OK' aura pour effet de chiffrer vos comptes et de vous en réserver l'accès.

Un clic sur 'Cancel' saute cette étape

Un clic droit sur l'application vous permet de renommer votre compte, de voir la clef secrète qui y est associée, de scanner le QR Code du compte.

Protection

Select how you would like to protect your authenticators. Using a password is strongly recommended, otherwise your data could be read and stolen by malware running on your computer.

Protect with my own password

Your authenticators will be encrypted using your own password and you will need to enter your password to open WinAuth. Your authenticators will be inaccessible if you forget your password and you do not have a backup.

Password:

Verify:

Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You MUST turn this off if you are going to reformat your disk, re-install Windows or delete this user account.

Encrypt to only be useable on this computer

And only by the current user on this computer

Lock with a YubiKey

Your YubiKey must support Challenge-Response using HMAC-SHA1 in one of its slots. Use the YubiKey personalization tool to configure the slot or click the Configure Slot button.

Slot 1:

Use Slot Configure Slot

OK Cancel

La durée de vie de la clef générée par WinAuth est de 30 secondes. A l'issue, vous pouvez demander l'affichage d'une nouvelle clef.