



IV. Solution de 2FA :

Pour la solution d'authentification à deux facteurs, nous avons choisi d'utiliser l'application microsoft authenticator. Le principe est simple, à l'ouverture de sa session, l'utilisateur doit s'identifier dans un premier temps avec ses identifiants de connexion Microsoft, puis valider la double authentification via à un smartphone, grâce à cette application.

Nous avons choisi cette solution car elle est facile à mettre en place et s'applique dès l'ouverture de la session windows. Enfin le fait d'utiliser une application comme microsoft authenticator nous permet si on le souhaite, de protéger d'autres services avec la même application. Par exemple, si un VPN est mis en place afin de pouvoir accéder au réseau de l'entreprise à distance (utile pour le télétravail), nous pouvons sécuriser son accès via une double authentification grâce à cette application.

L'inconvénient majeur de cette solution est que l'utilisateur doit obligatoirement avoir une connexion internet pour s'identifier. Mais elle présente d'autre inconvénients comme la nécessité de posséder une licence Windows Pro, ou encore le fait qu'elle crée une dépendance à une société américaine faisant partie des MAAMA

Actuellement, il existe un concurrent direct à microsoft authenticator, qui est google authenticator. Cependant, nous avons choisi l'application de microsoft pour les raisons suivante :

- Elle est protégé par un mot de passe.
- C'est un service proposé par Microsoft.

Processus d'identification

