Présentation générale sur les outils de télétravail au ministère de l'intérieur

Vous travaillez sur votre PC personnel. Vous disposez des outils suivants :

- **Nomade 2 :** un outil qui vous permet d'avoir accès à votre boîte mail professionnelle depuis votre PC ou téléphone personnel

- **TCHAP** : une messagerie instantanée réservée aux agents publics qui permet d'échanger à distance.

- **JITSI** : un service de webconférence interministériel permettant la coopération et travail à distance des agents publics issus des différents ministères.

- **Les supports amovibles** : les clés USB ou les disques durs externes qui permettent de transporter des documents non classifiés en télétravail.

- **Le centre d'appel au 01 40 07 20 00** qui vous accompagne en cas de difficultés.

Vous travaillez sur un poste NOEMI, un SPAN ou votre PC professionnel. Vous disposez des outils suivants :

- **SPAN** : Sécurisation des Postes d'Accès Nomades, qui permet hors de son lieu de travail habituel d'accéder à distance via une connexion internet ou le réseau du ministère à son environnement de travail (messagerie, dossiers locaux, ressources réseaux, etc…) comme si vous étiez au bureau.

  ou

- **NOEMI** : un ordinateur portable nomade sécurisé, raccordé à l'infrastructure du Ministère. En mode connexion, le poste offre les mêmes accès qu'un poste de travail. En mode hors-connexion, il est possible de travailler sur ses documents présents sur le portable.

- **COMU** : un outil de visioconférence sécurisée du Ministère de l'Intérieur. Il est accessible directement sur le poste de travail de l'agent et permet d'établir des visioconférences avec les agents du ministère de l'intérieur voire des utilisateurs externes au ministère moyennant la réservation d'un pont de visioconférence interministériel.

- **Le centre d'appel au 01 40 07 20 00** qui vous accompagne en cas de difficultés

Pour chaque outil vous trouverez dans ce guide des fiches d'utilisation vous permettant d'accéder à ces outils selon vos besoins.

SPAN

Sécurisation des Postes d'Accès Nomades

SPAN

Sécurisation des Postes d'Accès Nomades

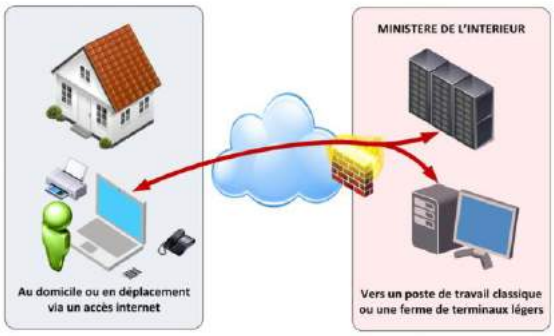
- ## Qu'est-ce que c'est ?

Le SPAN (Sécurisation des Postes d'Accès Nomades), permet hors de son lieu de travail habituel d'accéder à distance via une connexion internet ou le réseau du ministère à son environnement de travail (messagerie, dossiers locaux, ressources réseaux, etc…) comme si vous étiez au bureau et en toute sécurité.
La version 2 du SPAN permet notamment d'utiliser la solution COMU de visioconférence (cf. mode d'emploi ci après).
Contacter le 01 40 07 20 00 en cas de difficultés

- ## Qu'est-ce que cela permet ?

La solution de nomadisme SPAN du Ministère de l'Intérieur **offre une solution sécurisée d'accès distant aux infrastructures du Ministère**, qui permet :

- De prendre la main à distance sur son environnement de travail de façon totalement sécurisée,
- Depuis internet ou le réseau du Ministère,
- Par une liaison filiaire (Ethernet), Wifi (Box internet) ou 3G/4G (via un boitier Domino Airbox 3G/4G commercialisé par Orange dans le cadre du marché Opache 4),
- Se rapprocher de son référent SSI pour toutes questions complémentaires



Avant

J-7

Avant l'intervention du technicien

1. **Je demande à mon RSIM de vérifier si je remplie les prérequis NOEMI :**
   - **Possession de la carte agent**
   - **Certificats valides**
   - **Code PIN connu**
2. **Je dois effectuer la sauvegarde de mes données « Privées * » qui sont sur l'ordinateur, sur un support externe personnel (ex : clé USB, non fournie).**
3. **ATTENTION : Pour mes données « professionnelles » sur « C:\ » ou d'autres lecteurs LOCAUX , il faut les rapatrier sur :**

   Mon dossier « Mes Documents », pour préparer ma future sauvegarde de données.

* Les données « Privées », sont les données n'ayant aucun rapport avec votre activité professionnelle (exemples: courrier, musique, photos, vidéos …)

Pendant

Jour - J

Le jour de RDV avec le technicien

1. **Je dois être présent au DEBUT de l'installation et disponible pour une durée approximative de 2 heures.**
2. **Je valide avec l'informaticien mes dossiers à sauvegarder.**
3. **Je suis présent à la FIN de la migration avec l'informaticien pour contrôler avec lui que :**
   a. **Je peux me connecter avec mon mot de passe Windows.**
   b. **Puis je vérifie mes principales fonctionnalités.**
4. **Je remplis mon PV de Recette numérique avec l'informaticien.**

P.S. : Si je souhaite me connecter en 4G, je dois fournir la carte SIM le jour du RdV, pour que l'informaticien procède au paramétrage.

Après

Après J + 1

Après le passage du technicien

1. **Si je rencontre des difficultés avec Windows 10, je consulte :**
   - **Le triptyque de « PRISE en MAIN » ***
2. **Si j'ai un problème ou une demande (pour l'Administration Centrale), je fais un ticket avec**
   - **l'application « SETNA » ou**
   - **j'appelle « 72000 » au MI ou « 01-40-07-2000 » en dehors du MI.**

Je signale que je viens d'être migré(e) sur un NOEMI, et je précise mon site géographique :

Beauvau
Oudinot
Lumière
Lognes
Garance

* *Le Tryptique « PRISE en MAIN » sera envoyé par mail le Jour « J » de la migration.*

NOEMI

GUIDE UTILISATEUR

Préparation du déploiement du poste NOEMI

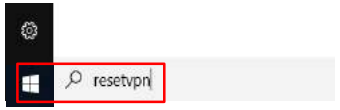
Aide VPN

Si vous rencontrez des problèmes de connexion, la première chose à effectuer est la suivante :

1. Dans la barre en bas de l'écran, observez l'icône de l'application VPN.

Si elle est bleu, exécuter les opérations ci-dessous.

2. Dans la zone « recherche », à droite du bouton « Démarrer », saisissez, « ResetVPN ».



3. Cliquez sur la procédure « ResetVPN » : l'outil fermera, puis relancera le VPN.

4. Après un laps de temps, l'icône de l'application VPN redevient verte.

5. Si le problème de connexion persiste, assurez vous que vous êtes bien connecté à un réseau (4g, filaire ou WIFI) et sinon contactez votre support informatique local.

Aide Carte Agent

Si vous avez un problème avec votre carte agent (oubli, perte, vol, certificat non valide…) et que vous ne pouvez pas utiliser votre PC, veuillez suivre les instructions suivantes :

1. Cherchez un collègue de votre direction et demandez-lui de « déverrouiller » votre PC, avec sa propre carte.
2. Si pas de collègue, appelez votre « Hotline » pour :
   - obtenir le mot de passe « CRYHOD », valable 1 mois.
3. Déverrouillez votre PC avec ce mot de passe CRYHOD.
4. Connectez-vous sur votre environnement Windows avec vos Login/Mot de Passe habituels, au lieu d'utiliser votre carte agent.
5. Si votre carte est perdue, volée ou défectueuse, demandez à la « Hot-Line » de dérouler la procédure de « Révocation/Renouvellement » de carte.

P.S. : Lorsque vous retirez la carte, le poste NOEMI se met « en veille ». Pour revenir dans votre session Windows, il faut remettre votre carte agent, saisir votre code PIN et saisir vos Login/MdP Windows.

Guide de prise en main du poste NOEMI

La solution NOEMI du Ministère de l'Intérieur offre un ordinateur ultra-nomade sécurisé. Il est connecté au travers d'un VPN sur l'infrastructure du Ministère et ses données sont protégées par une solution de chiffrement locale.

Renseignements

Si je rencontre des difficultés avec mon poste NOEMI :

- Je fais un ticket avec l'application « SETNA » ou j'appelle le « 72000 »

Le poste de travail NOEMI permet de bénéficier de la solution de visioconférence COMU !!!

MINISTÈRE DE L'INTÉRIEUR

DNUM

Aide connexion Wi-Fi

Pour vous connecter à un réseau Wi-Fi personnel (box personnelle, partage de connexion depuis un téléphone perso,…) veuillez suivre les instructions suivantes :

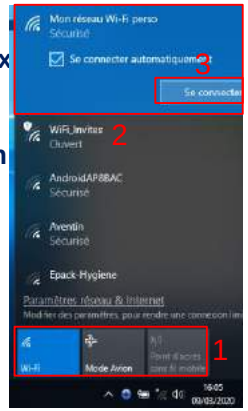
1. Assurez-vous que :

❑ Le VPN soit bien fermé (icône bleu en bas de la capture et le texte « Ouvrir » visible dans la fenêtre de connexion VPN)

❑ Vous soyez bien déconnecté de tout autre type de connexions. L'icône doit être présente sur votre écran.

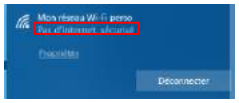
2. Ouvrez la fenêtre des réseaux en cliquant sur .

3. Assurez-vous que seule la section « Wi-Fi » est activée (en bleu). Si ce n'est pas le cas, faites un clic gauche sur les autres icônes en bleu.

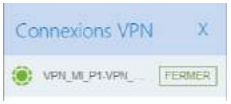


4. Cliquez sur votre réseau Wi-Fi, ici « Mon réseau Wi-Fi perso »

5. Cliquez sur « Se connecter »



La mention *« Pas d'internet sécurisé »* doit s'afficher après une connexion réussie. Réessayer si ce n'est pas indiqué.



Une fois connecté, relancez le tunnel VPN en cliquant sur « Ouvrir » dans la fenêtre de connexion.

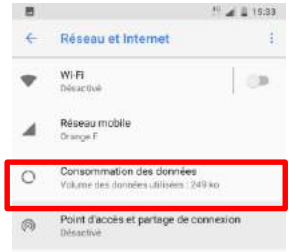
Partage de connexion

Si vous n'avez aucun Wifi, pas de câble réseau, pas d'accès à votre 4G via la carte SIM de votre NOEMI, vous avez encore la possibilité de faire un partage de connexion avec votre téléphone personnel.

Pour un Iphone

1. **Accédez à Réglages > Données cellulaires ou Réglages > Partage de connexion**
2. **Sélectionnez « Partage de connexion »**
3. **puis touchez le curseur pour l'activer.**

Pour un Android

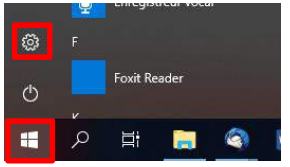


1. **Accédez à Paramètres Puis Réseau et internet**
2. **Sélectionnez ensuite sur « Point d'accès et partage réseau »**
3. **Enfin, activez le « Point d'accès mobile » ou « Point d'accès Wifi » (cela dépend de votre téléphone)**

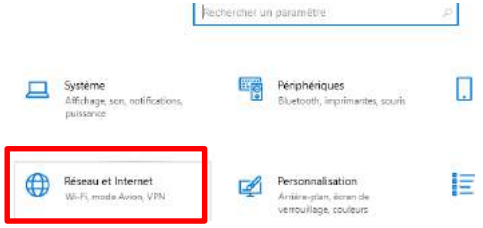
Aide 4G

Si vous rencontrez des problèmes de connexion au VPN ou une connexion ralentie en étant sur de la 4G, commencez par regarder vos informations de consommation :

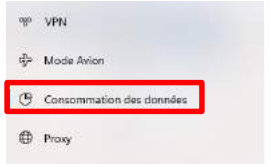
1. **Sur votre bureau, cliquer sur le bouton Windows et ensuite sur « Paramètres »**



2. **Dans la fenêtre qui s'affiche sélectionner « Réseau et Internet »**



3. **Cliquer sur « Consommation des données »**



4. **Vérifier le nombre de Go indiqué pour le « cellulaire », si ce nombre est > à 20Go, vous êtes en connexion bridée par l'opérateur.**

COMU

Un outil de web conférence sécurisée du MI

comU est accessible directement sur le poste de travail de l'agent afin de faciliter les échanges entre différents sites et/ou différentes directions du Ministère de l'Intérieur.

1 Je me connecte à l'Outil de Webconférence

- **Connectez-vous** à la webconférence via l'adresse https://webconf.comu.minint.fr
- Cliquez sur : **Se connecter**
- Entrez vos identifiants de connexion sous le format : **<domaine>-<login>@comun.minint.fr**
- Cliquez sur **« se connecter »**

Le domaine varie selon votre entité :
AC : Administration Centrale
AT : Administration Territoriale
PJ : Police Judiciaire
SP : Sécurité Publique
DG : Direction Générale
CRS : Compagnie Républicaine de Sécurité
PAF : Police Aux Frontières
PPOL : Préfecture de Police

Le login est : votre nom suivi des deux premières lettres de votre prénom
Mot de passe : votre mot de passe de session Windows
Exemple : pour Jean Dupont qui travaille en administration centrale ac-dupontje@comu.minint.fr

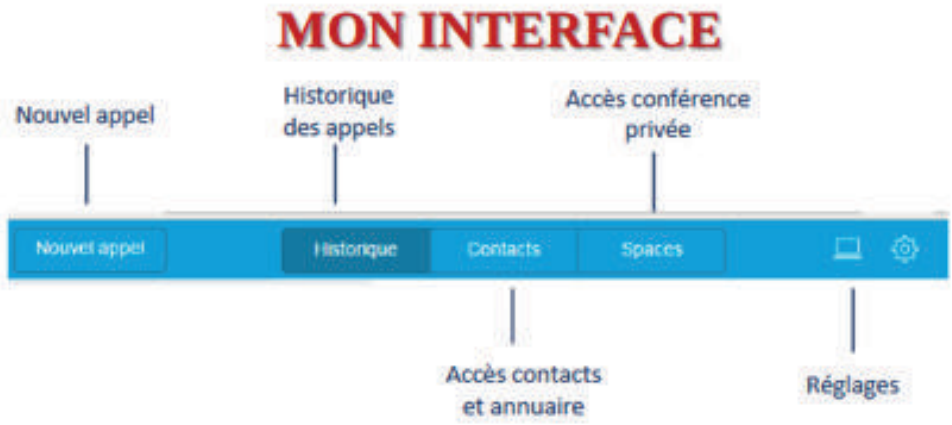
Pour la gendarmerie : prenom.nom@comun.mintint.fr
Mot de passe : votre mot de passe intranet
Exemple : jean.dupont@comu.minint.fr

COMU

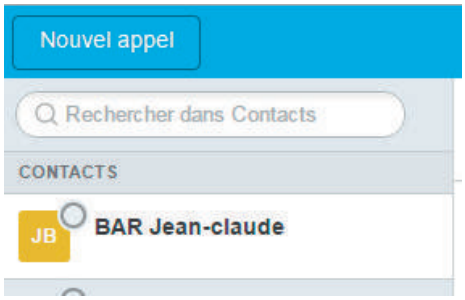
Un outil de web conférence sécurisée du MI

comU est accessible directement sur le poste de travail de l'agent afin de faciliter les échanges entre différents sites et/ou différentes directions du Ministère de l'Intérieur.

2 Mon Interface



3 Passer un Appel

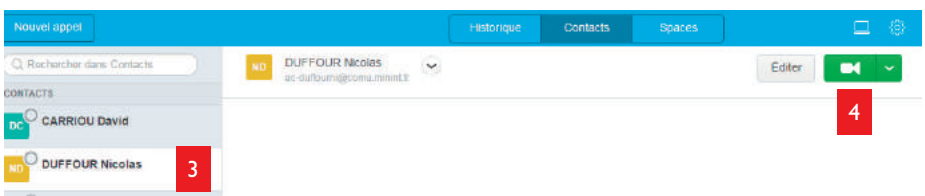


Onglet « Contacts

Même si la personne que vous souhaitez appeler ne fait pas partie de vos contacts, entrez son nom et son prénom dans Rechercher dans Contacts .

Si la personne recherchée ne fait pas partie de vos contacts, vous pouvez « Ajouter le contact» [1]. Pour l'appeler, cliquez sur la caméra verte [2].

Si la personne recherchée fait partie de vos contacts, cliquez sur son nom dans la liste [3]. Pour l'appeler, cliquer sur la caméra verte [4].



NOMADE 2

- ## Qu’est-ce que c’est ?

Cet outil vous permet de consulter votre boite professionnelle depuis votre ordinateur familial personnel

- ## Quelle est la procédure pour bénéficier du service ?

Dans le cadre de la procédure exceptionnelle « COVID-19 », cette phase de création est automatisée et les agents concernés recevront directement les certificats permettant leur connexion.

Afin de bénéficier du service, il faut suivre la procédure suivante :

1. **Contacter votre RSSI (et uniquement votre RSSI)** qui initiera la création ou le renouvellement de votre accès avant votre confirmation depuis CAPITOLE (cf paragraphe "Comment demander un accès au service NOMADE2" de la FAQ CAPITOLE disponible ici : http://ssi.minint.fr/index.php/faq-capitole)

2. Activer l'**accès Hesperis** sur le compte Icasso (case à cocher “Accès Hesperis” au niveau du compte de l'utilisateur - Seul votre gestionnaire messagerie peut réaliser cette opération – Fait par défaut dans le cadre du COVID 19 – En cas de difficultés, contacter le 01 40 07 20 00).

Attendre **1h15** maximum après sa validation pour exécuter le paramétrage.

Une fois que vous aurez reçu les deux mails vous fournissant vos identifiants de connexion, le service pourra être mis en place.

Mise en place du service

Avant de procéder à la génération des certificats, veuillez vous assurer de la bonne réception du mail de confirmation du service service Nomade2 (charte-nomade2@interieur.gouv.fr)

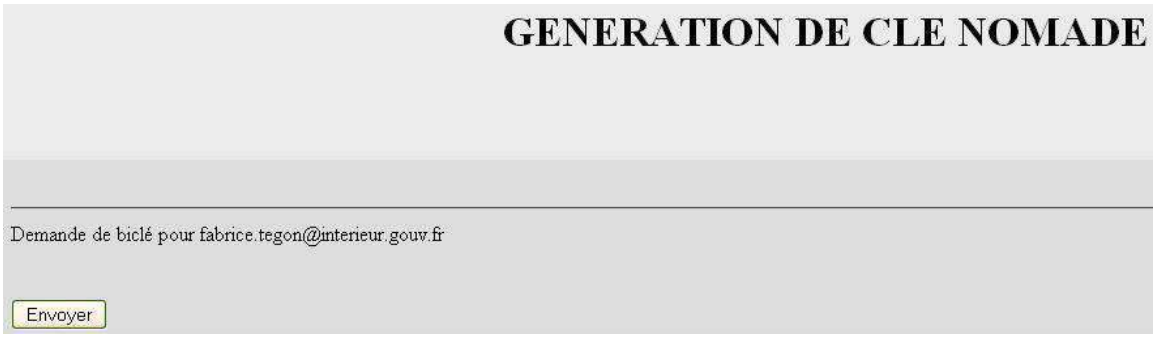
Dans le cadre de la procédure exceptionnelle « COVID-19 », la première phase est généralisée et seule les phases 2 et suivantes décrites ci-dessous sont à appliquer.

1- Génération d'un **certificat personnel** en se connectant, depuis le RGT, sur le site: https://certif.messagerie.si.mi/

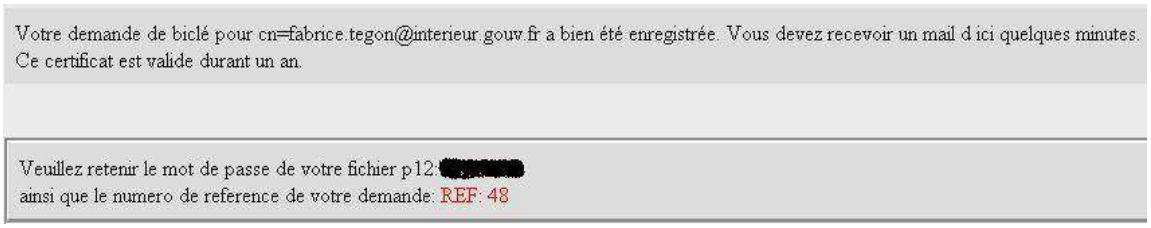
2- La bannière suivante s'ouvre :

3- Entrer comme login l'**adresse mail** (adresse **métier** en @interieur.gouv.fr ou en **departement.pref.gouv.fr**) + le **mot de passe** de connexion à la messagerie **Icasso**.

4- La page suivante s'ouvre pour **valider** l'envoi du **certificat** (cliquer sur “Envoyer”) :



5- Un **mot de passe** est alors **indiqué à l'écran**, il faut le noter car il sera demandé lors de l'**installation du certificat** au format p12 sur la machine utilisée pour l'accès à **Nomade 2**. Vous pouvez également noté la référence du certificat :



6- Après génération du certificat, **2 messages sont envoyés à l'utilisateur**, l'un contient en pj une autorité de certification, l'autre contient (également en pj) le certificat personnel de l'utilisateur.

7- Ces 2 certificats doivent alors être **installés** dans le **navigateur web** de la machine depuis laquelle l'utilisateur accédera au service **Nomade 2**.

8- La procédure d'installation des certificats ainsi que l'adresse du webmail sont indiquées dans le message d'envoi du certificat personnel.

Une **documentation complète** sur l'installation des certificats se trouve ICI (http://messagerie.dsic.minint.fr/Fichiers/Documents/Nomadisme/Nomade2/Presentation/Installation_certificats_nomade2_modif.pdf).

Celle-ci peut s'avérer utile pour toute installation des certificats sur les PC personnels au domicile des autorités.

URL de connexion au service : **https://msg.interieur.gouv.fr**

IMPORTANT : Lors de l'affichage du mot de passe associé au certificat, si ce dernier contient un point ou tout autre caractère spécial en début, milieu ou fin de chaîne (= - _ ? !), ceux-ci font partie du mot de passe. Il faudra donc les saisir pour procéder à l'installation du certificat.

Par ailleurs, veillez bien à ne pas confondre les chiffres et les lettres (1 et la lettre l en minuscule, zéro et la lettre O par exemple).

ATTENTION, toute connexion au site sans les certificats installés entraînera une erreur au niveau du navigateur.

DOCUMENTATION UTILISATEUR Nomade 2 : ICI (http://messagerie.dsic.minint.fr/Fichiers/Documents/Nomadisme/Nomade2/Presentation/Utilisation_du_webmail_nomade_2.pdf).

LES SUPPORTS AMOVIBLES

- ## Qu'est-ce que c'est ?

Les supports amovibles tels que les clés USB ou les disques durs externes permettent de transporter des documents non classifiés en télétravail.

- ## Quelle est la procédure à suivre ?

Étape 1 : Dans un premier temps, chaque structure achète dans le commerce les supports amovibles dont elle a besoin.

Dans un second temps deux cas de figure peuvent se présenter :

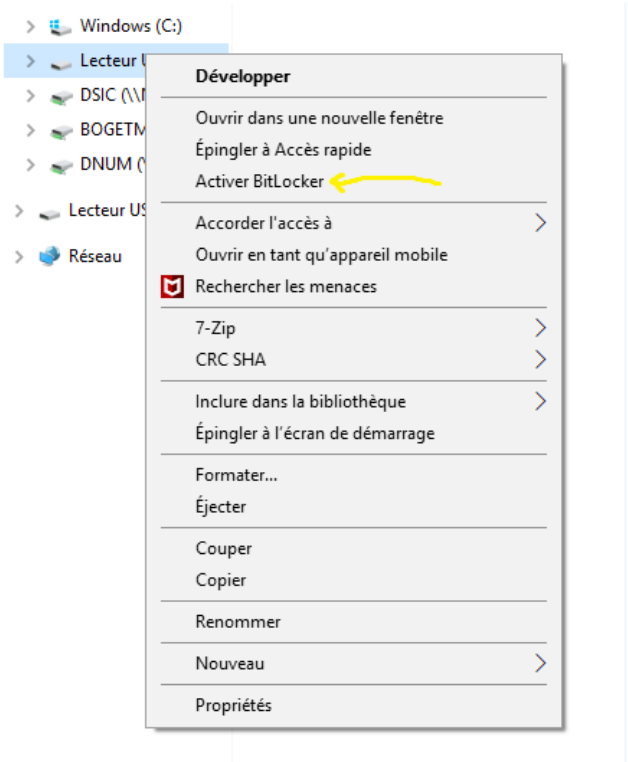
- ***Premier cas de figure :*** La protection empêchant le raccordement de supports amovibles non déclarés aux PC du ministère est actuellement activée par le RSSI de la structure. Il faut alors prendre contact avec le RSSI pour que celui-ci déclare les supports amovibles acquis comme étant raccordables à des PC professionnels.

- ***Deuxième cas de figure :*** La protection empêchant le raccordement de supports amovibles non déclarés aux PC du ministère n'est pas actuellement activée. Il faut alors passer directement à l'étape 2.

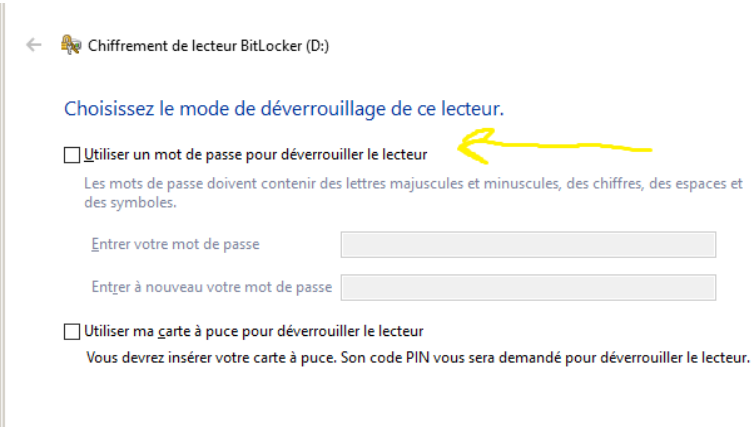
Étape 2 : De manière à garantir un minimum de **confidentialité et de protections des données** qui, sans être classifiées, peuvent être potentiellement sensibles, i**l faut activer BitLocker sur la clé qui a été insérée** (cf mode d'emploi ci-dessous)

- **Mode d’emploi pour activer BitLocker sur la clé USB insérée :**

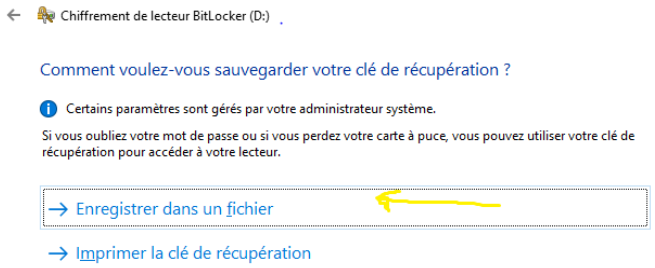
1. **Cliquer dans « Lecteur » puis cliquer sur « Activer BitLocker »**



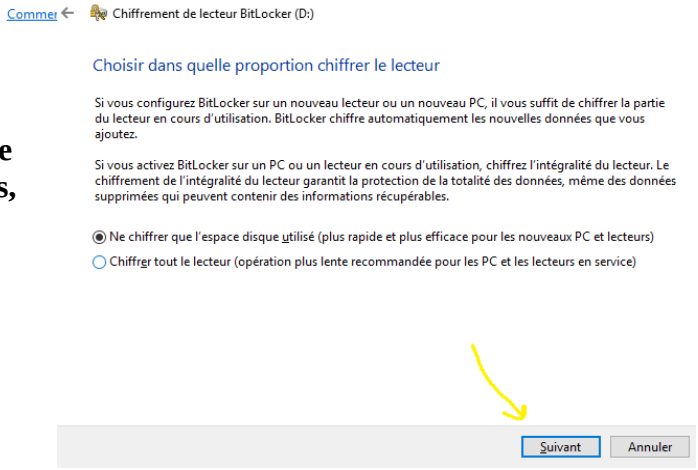
2. **Cliquer sur « Utiliser un mot de passe pour déverrouiller le lecteur ». Puis, créer un mot de passe que vous entrerez deux fois.**



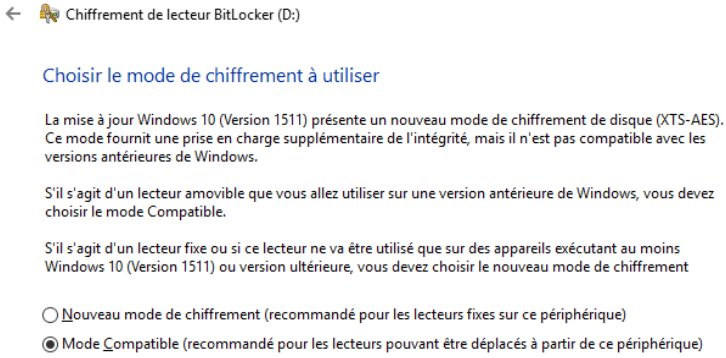
3. **Cliquer sur « Enregistrer dans un fichier »**



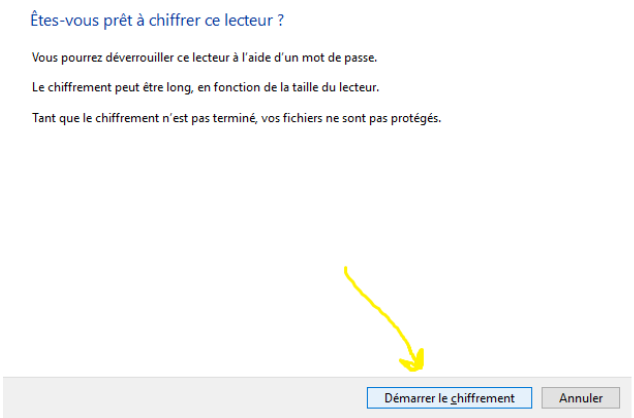
4. **Cliquer sur « Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs) ». Puis, cliquer sur « Suivant »**



5. **Cliquer sur « Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique) »**



6. **Cliquer sur « Démarrer le chiffrement »**



Les utilisateurs de postes personnels Linux comme ceux rencontrant des difficultés avec la procédure prendront contact avec leur RSSI.

TCHAP

La messagerie instantanée des agents publics

Rejoignez les **85 000** agents déjà utilisateurs !

DISPONIBLE SUR Google Play

Télécharger dans l'App Store

Et en version web sur tchap.gouv.fr

TCHAP
La messagerie instantanée des agents publics

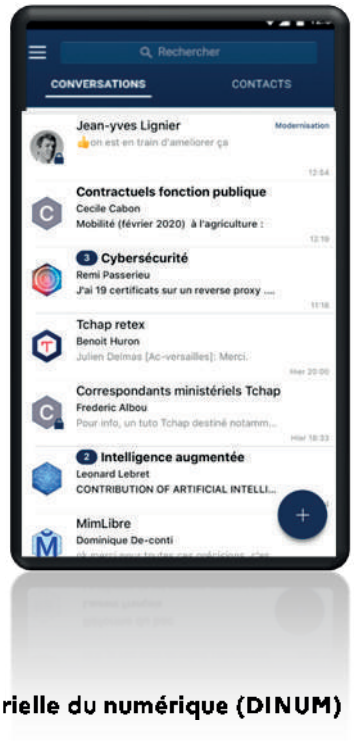
Pour vos échanges à distance, vous pouvez compter sur Tchap, la messagerie instantanée créée pour les agents publics, opérée par l'État.

À QUOI ÇA SERT ?

- **Discuter en privé à deux ou en groupe** (salon), avec un agent en télétravail
- **Partager des fichiers** (documents, photos, vidéos…)
- **Inviter des correspondants extérieurs** à l'État (partenaire, prestataire…) à ungroupe
- Créer ou rejoindre des **groupes de discussion publics,** ouverts à tous
- Retrouver facilement un interlocuteur grâce à l'**annuaire intégré des utilisateurs...**

COMMENT L'UTILISER ?

- Tchap est disponible **sur smartphones** (Android et Apple) et **sur ordinateur** via un simple navigateur
- Tout agent peut s'inscrire à partir de **son adresse mail professionnelle**



EN TOUTE SÉCURITÉ

- Solution hébergée sur les **serveurs de l'État**
- **Échanges chiffrés** de bout en bout (hors salons publics)
- **Analyse antivirus** des fichiers partagés
- **Service homologué** par la DINUM

En savoir plus

Un service proposé par la direction interministérielle du numérique (DINUM)

JITSI

Webconférences de l'État

Rejoignez les **12 000** participants mensuels !

Accéder à webconf.numerique.gouv.fr

Webconférence de l'État

pour vos réunions à distance

Webconf.numerique.gouv.fr permet notamment d'**organiser en ligne, à distance, des réunions, des conférences, des présentations.**

À QUOI ÇA SERT ?

- **Organiser une réunion à distance en audio et vidéo,** avec des collaborateurs en télétravail par ex
- **Diffuser une présentation**
- **Partager la fenêtre d'un programme** sur votre ordinateur
- **Discuter en instantané** via un tchat intégré
- **Éditer un texte en mode collaboratif** et en temps réel…

COMMENT L'UTILISER ?

- **Matériel nécessaire :** webcam, micro et hauts-parleurs (ou, mieux, un casque avec micro intégré)
- **Pour créer un salon,** se connecter depuis le réseau de l'État (RIE)
- **Pour rejoindre un salon,** se connecter depuis n'importe quel ordinateur

EN TOUTE SÉCURITÉ

- Solution hébergée sur les **serveurs de l'État**
- **Données chiffrées** via un protocole sécurisé

En savoir plus

Un service proposé par la direction interministérielle du numérique (DINUM)

5 BONNES PRATIQUES POUR UN USAGE D'INTERNET EN TÉLÉTRAVAIL

LORSQUE J'UTILISE MA CONNEXION À DISTANCE :

1 **JE RÉSERVE**
mes consultations internet à un usage strictement professionnel

2 **J'ÉVITE**
les téléchargements de fichiers lourds ET les accès aux espaces de stockage distants (drives)

3

JE SUPPRIME
les images de ma signature de mail ou la réduis au strict nécessaire (nom, prénom, numéro de téléphone)

4

JE ME DÉCONNECTE
du réseau à distance ou utilise mon ordinateur ou mon smartphone personnels :

- ➔ pour des usages gourmands comme le visionnage de vidéos non sensibles
- ➔ pour des recherches/consultations

J'applique ces bonnes pratiques
c'est la garantie pour tous de préserver l'accès à nos outils informatiques

Des recommandations de la direction interministérielle du numérique (DINUM)