107

Concours interne
Ingénieur des SIC

Matière : Cas pratique

Date : 30/05/2017

Nombre d'intercalaires : 1

17/60

Rabattre ici le coin gommé

NOTE	ANNOTATIONS :
/20	

NOTE DE CADRAGE

Objet : Mise en place du télétravail

Depuis la parution de l'arrêté du 02 mars 2017 relatif au télétravail, il est possible, à nouvelles conditions, pour certains personnels des ministères de l'intérieur et des actionnaires de bénéficier de ce dispositif.
Le télétravail permet à un agent de pouvoir accéder au système d'information du ministère depuis son domicile ou lors de déplacements nationaux ou internationaux.
Cette note de cadrage s'inscrit dans un contexte où une cinquantaine d'agents ont exprimé le désir de pouvoir bénéficier de ce nouveau dispositif. Après avoir présenté le télétravail, aux niveaux réglementaire, organisationnel et technique, nous verrons en détail le plan de déploiement à mettre en œuvre, en balayant les aspects techniques, budgétaires mais également les risques encourus, la formation et ~~la~~ communication pour finir par la planification globale du projet.

[redacted]

I) Le télétravail

a) définition

Le télétravail est le dispositif permettant à un agent d'accéder au système d'information des ministères de l'intérieur et des outre-mer depuis son domicile ou en déplacement. Pour cela le dispositif s'appuie sur une solution technique, le poste nomade qui sera détaillé dans la partie c de ce chapitre, mais également sur des textes réglementaires que nous allons à présent présenter.

b) La réglementation

La mise en œuvre du télétravail au sein des ministères de l'intérieur et des outre-mer est possible et encadrée par le décret n° 2016-151 du 11 février 2016 et plus particulièrement de l'arrêté du 22 mars 2017 portant application du décret cité plus haut.

Cet arrêté est applicable aux agents publics civils affectés dans un service du ministère de l'intérieur, dans l'un des établissements publics relevant de la tutelle administrative du ministère de l'intérieur ou dans un service du ministère chargé des outre-mer. Toutefois, l'arrêté liste un grand nombre d'activités exclues exclues du périmètre d'éligibilité du télétravail. En voici une liste non-exhaustive :

- activités opérationnelles, de représentation de l'État, nécessitant un accueil physique
- accomplissement de travaux confidentiels ou données sensibles
- accomplissement de travaux au travers de logiciels faisant l'objet de restriction ou non éligible au télétravail à distance

- accomplissement de travaux nécessitant le déplacement sur un autre lieu que le lieu de travail habituel.

L'article 3 de l'arrêté précise que le télétravail s'organise au domicile de l'agent ou dans un télécentre, sous réserve qu'une convention ait été conclue avec le responsable du télécentre.
Cet article ainsi que les suivants ~~de l'arrêté~~, font mention de l'aspect technique et organisationnel du télétravail.

c) Aspects techniques et organisationnels

1) Aspects organisationnels

Bien que n'étant pas sur leur lieu de travail, les agents en télétravail sont tout de même soumis à la même réglementation, à la fois en matière d'hygiène et de sécurité mais également en matière de temps de travail.
Chaque service concerné par le télétravail doit travailler dans le document unique d'évaluation des risques professionnels la prévention des risques professionnels liés au télétravail. En outre, la délégation du comité d'hygiène, de sécurité et des conditions de travail (CHSCT) a la possibilité de réaliser une visite sur le lieu d'exercice des fonctions en télétravail des agents.
Pour ce qui est du temps de travail, les agents en télétravail sont soumis à la réglementation en vigueur dans le service où ils exercent leurs fonctions. Les modalités de comptabilisation du temps de travail sont celles prévues dans le règlement intérieur du service d'affectation.

2) Aspects techniques

Le télétravail ne peut être possible qu'au travers d'une connexion internet et l'usage d'un poste informatique. Ce dernier est mis à disposition par l'administration et doit respecter les spécificités techniques définies par la direction des systèmes d'information et de communication du ministère de l'intérieur. Ce poste nomade est plus communément appelé poste SPAN. Il peut être attribué à un service et servir pour plusieurs utilisateurs. En effet son usage est contrôlé via un "token personnel", sorte de clé usb personnelle contenant les informations d'

d'identification et d'authentification de l'usager.
En annexe de l'autorisation individuelle d'accès des fonctions en télétravail se trouve la charte portant engagement des utilisateurs du service de sécurisation des postes d'accès nomade.
Le poste SPAN est ainsi un poste informatique sécurisé qui permet, au travers d'une connexion internet (Ethernet, wifi, 3G/4G), d'accéder à son environnement de travail de façon totalement sécurisée.

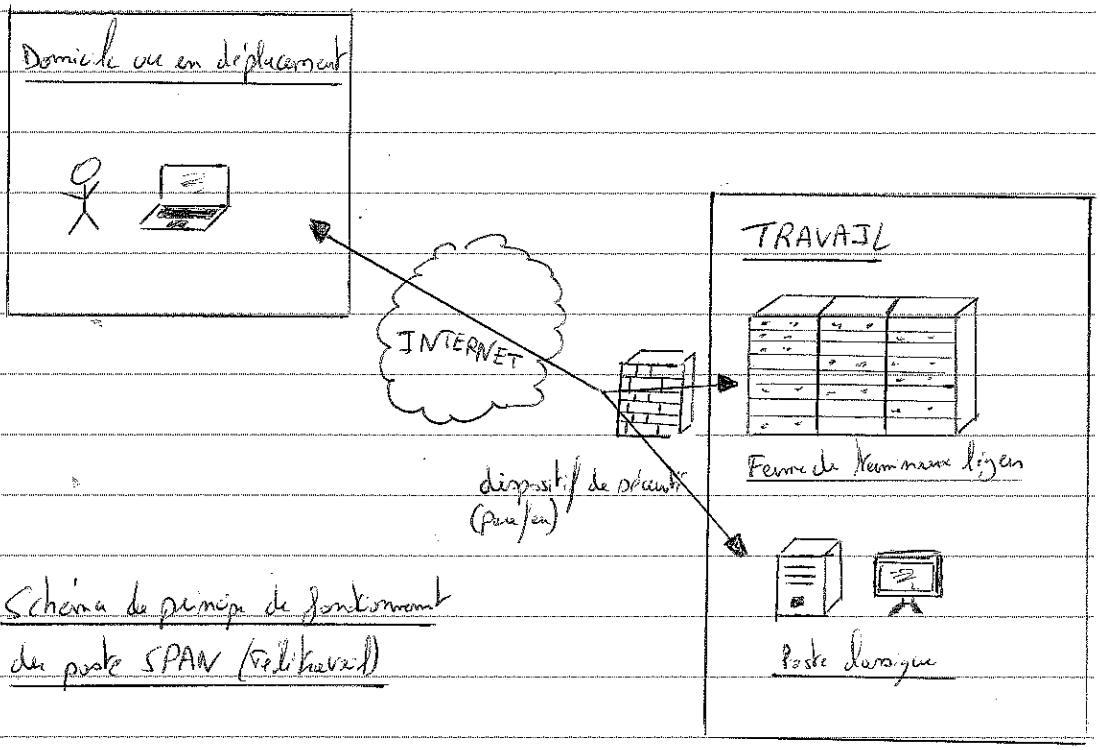


Schéma de principe de fonctionnement du poste SPAN (Télétravail)

Le schéma ci-dessus nous présente le principe de fonctionnement général du poste nomade (poste SPAN). Au travers d'une simple connexion internet il est possible d'accéder de manière sécurisé, grâce au post. SPAN et aux dispositifs de sécurité des ministères (pare-feu, VPN), à son environnement de travail.

Nous allons à présent exposer le plan de déploiement des dispositifs de télétravail pour les agents

c) Aspects budgétaires

L'utilisation de poste nomade n'est pas sans impliquer un coût d'acquisition. Il existe plusieurs type de postes, en fonction de leur configuration et performance. Deux types nous intéressent :

- poste standard
- poste ultra-book.

Le premier (standard) a un coût d'acquisition de 649,55 HT, le second 819,70€ HT. A ce coût initial doit s'ajouter l'achat des tokens (un par usager) : 65€ HT par token.

Dans l'optique d'équiper chaque agent du premier poste le coût total d'acquisition s'élève à 30 000€ HT environ, alors que pour le second le total avoisine d'environ 45 000€ HT.

A cela il sera potentiellement nécessaire d'ajouter le matériel dont l'ouïe aura relevé l'importance pour rendre notre S.I compatible avec le télétravail.

Dans certains cas, l'administration devra également fournir une connexion nomade aux usagers en déplacements. Il faudra alors consulter le marché OPALINE 4 pour trouver le matériel nécessaire et le commander.

d) Formation et communication

La mise en place d'un tel dispositif passe par une campagne de communication, à destination de tous les services et usagers potentiels afin de rappeler le cadre légal et réglementaire mais également de les sensibiliser aux risques et dangers potentiels.

En outre, la campagne de communication sera un bon moyen de recenser les usages et services désirés du dispositif ainsi que leur usage.

Une fois le dispositif en place et prêt techniquement, des sessions de formation seront dispensées aux usagers du dispositif télétravail.

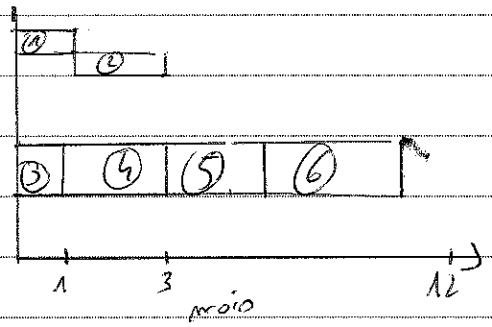
Ces formations auront pour objectif de le former à la prise en main du poste SPAN ainsi que de les sensibiliser aux les dangers potentiels (perte de matériel, virus...) et les différentes règles SSI à respecter.

Une formation technique sera également prévue pour former les techniciens sur le dépannage ainsi que l'exploitation des traces (fichiers journaux) en cas d'incident avec le dispositif.

e) Analyse des risques

Dans le cadre de l'analyse des risques il est nécessaire d'identifier les risques potentiels pouvant entraîner un impact négatif sur le projet.
Sur le plan organisationnelle il faudra s'assurer que tous les pré-requis définis dans l'arrêté soient respectés, y compris la transmission de différentes pièces justificatives et attestation par l'usager (connexion internet, pièce bureau au domicile...).
Sur le plan technique, on veillera à la sensibilisation des usagers pour les risques SSI mais également contre la perte ou le vol des matériels nomade.
On s'assurera que le SI est bien préparé au télétravail pour le mise en place d'une traçabilité des connexions, des actions, une redondance des équipements informatiques et électriques

f) Planification



① Audit du S.I (1m)
② Mise en conformité du SI (2m)
③ recensement besoin usager et service (1m)
④ Commande et préparation poste SPAN (2m)
⑤ Communication et formation poste SPAN (2m)
⑥ Mise en place et activation du dispositif (1m)

Le dispositif télétravail sera opérationnelle sous neuf mois environ et ainsi le durée de mise en place initiale de 12 mois sera respectée. Par ailleurs le delta de 3 mois prévu servira en cas de pics imprévus.

II) Plan de déploiement du dispositif télétravail.

Le déploiement du dispositif télétravail impose une implication de plusieurs services, directions, afin qu'il puisse être mis en œuvre au sein de notre structure.
En effet, l'implication des ressources humaines, des services administratifs et financiers, du CHSCT ou encore des services informatiques sera nécessaire, comme nous l'a montré la première partie de cette note.
Avant de détailler la solution technique, l'aspect budgétaire, l'analyse de risque ou encore la formation et communication, une analyse de l'existant reste incontournable.
et des besoins

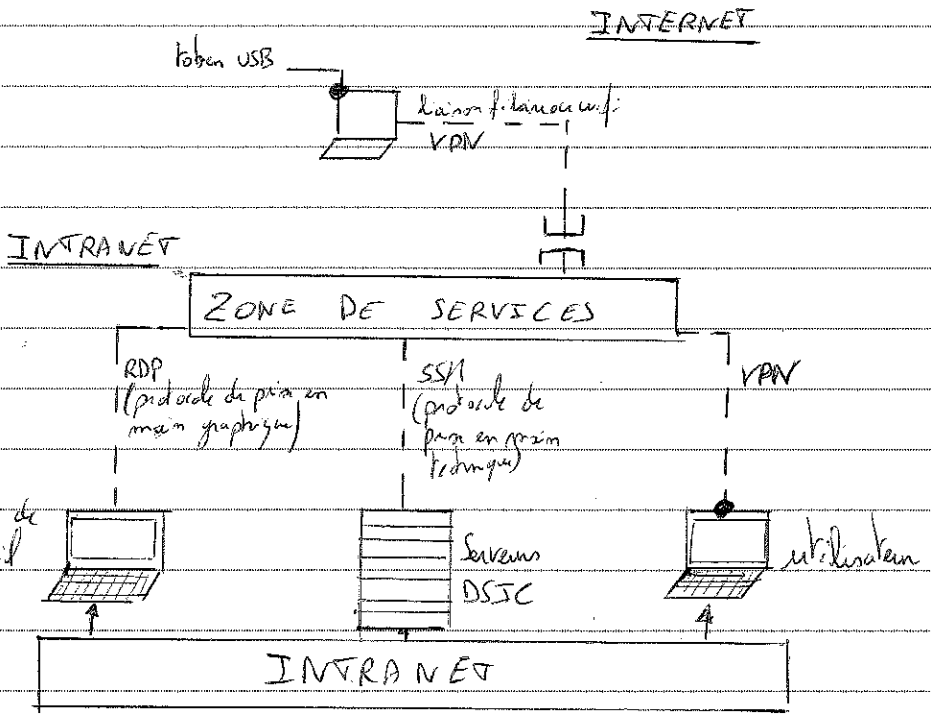
a) Etat initial

Avant d'entamer les changements ou procédures nécessaire à la mise en place de télétravail, il est important de faire un état des lieux du système d'information actuel dans son ensemble.
L'objectif est d'analyser le système d'information dans le but de vérifier si en l'état il est compatible avec l'arrivé du dispositif de télétravail.
Pour réaliser cet audit, nous pourrons demander l'appui technique de la chaine SSI (Sécurité des Systèmes d'Information) ainsi que de l'A.N.S.S.I (Agence Nationale de la Sécurité des Systèmes d'Information) qui pourra être désigné AMO (Assistant à la maîtrise d'ouvrage) pour ce projet.
Cet audit devra mettre en correspondance les besoins nécessaires à ce dispositif, l'état actuel du S.I. et les actions à mener pour rendre notre S.I (système d'information) éligible au dispositif télétravail.

b) Solution technique

Citée plus haut, la solution d'accès à distance pour le télétravail est le poste SPAN. Il s'agit d'un poste informatique nomade (portable) sécurisé.
Le poste établit une communication sécurisée au travers d'un tunnel chiffré (VPN) vers les infrastructures du ministère. La communication s'établit par internet, soit en 3G/4G via un smartphone soit par une box ADSL en place chez l'utilisateur.
Une fois la communication établie l'utilisateur accède à son propre poste de travail

ou à un environnement virtuel de travail.
Le principe technique sous-jacent de la solution consiste en un déport d'écran de l'environnement de travail de l'utilisateur vers le poste nomade.
Ce déport est sécurisé par de nombreuses couches techniques et optimisé en terme de débit.
Par ailleurs l'accès à un poste SPAN est assujetti à l'emploi d'un token personnel.
Cette solution implique que le S.I dispose d'une zone de service permettant ces accès distants.



Architecture technique du poste SPAN

Le poste SPAN permet ainsi de protéger l'accès au S.I. du ministère et de l'établissement, grâce à sa méthode de connexion (VPN) et d'authentification (token USB).
Le VPN permet une sécurisation de bout en bout de la communication établie grâce au cryptage des données, au filtrage des paquets, à l'authentification ainsi que son support multiprotocole.