

CONCOURS INTERNE ET 3E CONCOURS D'INGÉNIEUR DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2023 -

Mercredi 15 mars 2023

Concours interne :

Résolution d'un cas pratique à partir d'un dossier à caractère technique permettant d'apprécier les qualités d'expression, d'analyse et de synthèse du candidat et sa capacité à conduire un projet.

3e concours :

Résolution d'un cas pratique à partir d'un dossier à caractère technique faisant appel à des connaissances relatives à l'environnement et à la technique des systèmes d'information et de communication et permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 4 heures – Coefficient 1)

**Le dossier technique comporte 33 pages.
(hors page d'énoncé du sujet).**

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entraînera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A ..., B..., Y..., Z...).

IMPORTANT

- 1. LES COPIES SERONT RENDUES EN L'ÉTAT AU SERVICE ORGANISATEUR. A L'ISSUE DE L'ÉPREUVE, CELUI-CI PROCÉDERA À L'ANONYMISATION DE LA COPIE.**
- 2. NE PAS UTILISER DE CORRECTEUR OU D'EFFACEUR SUR LES COPIES.**
- 3. ÉCRIRE EXCLUSIVEMENT EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.**
- 4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAÎTRE SUR LA COPIE.**

SUJET

Lors du comité interministériel à la transformation publique du 23 juillet dernier à Vesoul, le Premier ministre a annoncé poursuivre la démétropolisation des services de l'État et leur relocalisation dans les territoires.

En qualité de chargé de mission au sein de la direction du numérique du ministère de l'Intérieur et des Outre-mer, vous devez conseiller la cheffe du bureau du recrutement de la DRH dont le service doit être délocalisé dans une ville moyenne de la région Nouvelle-Aquitaine.

Ce projet prévoit l'installation de 50 agents sur un étage dédié de 400m² (dont 100m² de salles de réunion) d'un immeuble privé, doté d'espaces de travail partagé, adapté pour un usage administratif et pouvant accueillir simultanément 30 personnes au maximum. Le télétravail sera favorisé, sur la base du volontariat, et les échanges en distanciel, tant avec l'administration centrale qu'avec les partenaires privés devront être assurés de façon fluide et sécurisée.

À l'aide du dossier technique joint et de vos connaissances personnelles, vous rédigerez une note argumentée (5 pages maximum) précisant les ressources numériques nécessaires au bon fonctionnement de cette nouvelle entité dès le 1^{er} janvier 2025.

Dans le respect des mesures relatives à la sécurité des systèmes d'information (SSI), vous proposerez des solutions pour répondre aux besoins identifiés dans les domaines suivants :

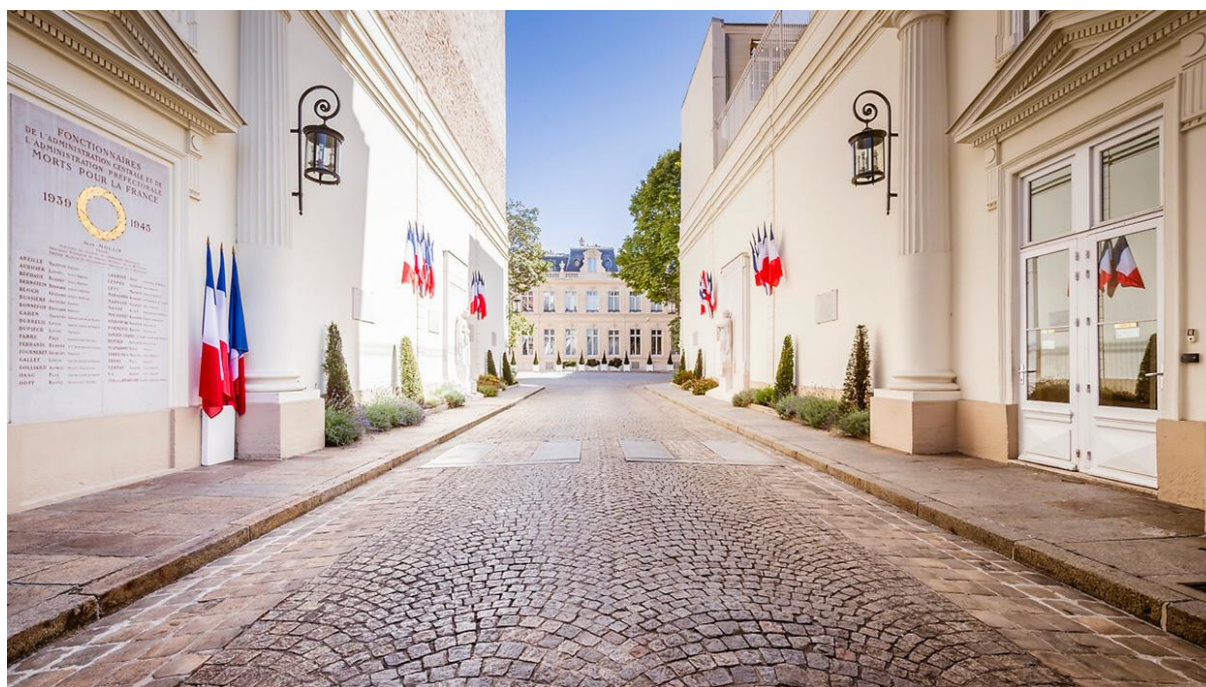
- Contrôle d'accès ;
- Architectures réseau et informatique ;
- Environnement de travail numérique de l'agent :
 - * postes de travail ;
 - * téléphonie ;
 - * applications métiers ;
 - * outils collaboratifs.
- Soutien utilisateur.

Votre note devra également intégrer les composantes organisationnelles et le phasage du projet, ainsi que l'accompagnement au changement.

Dossier technique :

Document 1	20 villes retenues pour accueillir des services d'administration centrale du ministère de l'Intérieur Source : Site institutionnel du ministère de l'intérieur. Publié le 16/03/2022	Page 3
Document 2	Gérer ses réseaux informatiques : comment agencer les bureaux ? Source : https://www.associationeconomienumerique.fr/gerer-reseaux-informatiques-agencer-bureaux/	Pages 4 et 5
Document 3	5 bonnes raisons de passer au Softphone Source : https://www.linkt.fr/blog/5-raisons-adopter-softphone-telephonie-entreprise/	Pages 6 et 7
Document 4	2021 – L'offre Startmiup v3.7 Source : Document interne, DNUM du Ministère de l'Intérieur	Pages 8 à 10
Document 5	Au ministère de l'Intérieur, la crise donne "un coup d'accélérateur" aux projets numériques et cyber Source : https://www.aefinfo.fr/depeche/626871-au-ministere-de-linterieur-la-crise-donne-un-coup-d-accelereur-aux-projets-numeriques-et-cyber	Pages 11 et 12
Document 6	Présentation de l'accord-cadre A07 de téléphonie fixe Source : http://dnum.minint.fr/index.php/telephonie/telephonie-fixe/information-s-generales/4261-00-documents-contractuels	Pages 13 et 14
Document 7	Deuxième chapitre – La conduite du processus des projets informatiques Source : Cours de méthodes de conduite des projets informatiques – YENDE RAPHAEL Grevisse	Pages 15 à 18
Document 8	ComU, l'outil de visioconférence du ministère de l'Intérieur Source : Document interne, DNUM	Page 19
Document 9	La ToIP, une solution de téléphonie d'entreprise à envisager au plus vite ! Source : https://www.elit-technologies.fr/la-toip-une-solution-de-telephonie-dentreprise-a-envisager-au-plus-vite/	Pages 20 et 21
Document 10	Produits numériques partagés Source : numerique.gouv.fr	Page 22
Document 11	Plaquette NOEMI DR et NOEMI SANS CARTE / ordinateur portable « Ministère de l'Intérieur » Source : Document interne, DNUM	Pages 23 et 24
Document 12	Le RIE, un réseau efficace en trois composants, performant et évoluant en trois axes. Source : Document interne ministère de la transformation et de la fonction publiques	Pages 25 à 28
Document 13	Contrôle d'accès RFID : qu'est-ce que c'est et comment ça marche ? Source : https://www.rfidfuture.com/fr/rfid-access-control.html	Pages 29 à 31
Document 14	Extrait du décret 2016-151 du 11 février 2016 relatif aux conditions et modalités de télétravail dans la fonction publique et la magistrature. Source : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032036983	Pages 32 à 35

20 villes retenues pour accueillir des services d'administration centrale du Ministère de l'Intérieur



Lors de son déplacement à la préfecture de Corrèze en septembre 2021, Gérald Darmamin, ministre de l'Intérieur, avait annoncé que des agents du ministère, en poste en Ile-de-France, seraient réinstallés dans des villes candidates à les accueillir.

Cette initiative faisait suite au comité interministériel à la transformation publique du 23 juillet dernier à Vesoul, lors duquel le Premier ministre avait annoncé poursuivre la relocalisation des emplois hors de l'Ile-de-France, hors des grandes métropoles.

Le souhait du Président de la République et du Gouvernement est ainsi de contribuer à renforcer la proximité de l'État avec les Français, d'offrir une opportunité pour les villes qui accueilleront ces nouveaux emplois et de répondre à l'aspiration de nombreux agents de l'État de travailler dans un autre cadre de vie.

Le ministère de l'Intérieur a reçu de très nombreuses candidatures de villes disposées à accueillir l'un des 20 services de l'État destinés à se relocaliser, issus de l'administration centrale du secrétariat général du ministère, de la direction générale de la Police nationale, de la direction générale de la Gendarmerie nationale, de la direction générale de la sécurité civile et de la gestion des crises et de la délégation à la sécurité routière.

Ces candidatures ont été examinées à partir d'une grille de critères tenant compte de l'offre immobilière, mais aussi du cadre de vie, de la mobilisation locale autour du projet, et de l'appui que pourrait apporter cette implantation pour soutenir le développement local.

Gérer ses réseaux informatiques : comment agencer les bureaux ?

Du fait d'une augmentation de la taille de votre entreprise, il peut arriver que vous soyez contraint de déménager pour aller occuper des locaux plus grands. Parmi les nombreux défis qui vous attendent, l'installation du réseau informatique est une priorité. Le but de ce mini-guide est de vous aider à mettre en place un réseau informatique dans votre entreprise en tenant compte de l'agencement de vos bureaux.

Les étapes de la mise en place d'un réseau informatique

La première étape consiste à définir vos besoins en informatique. La superficie globale du lieu de travail, les caractéristiques techniques, le nombre des machines nécessaires (postes individuels et serveurs) sont autant d'éléments qui seront mentionnés dans le cahier des charges.

La deuxième étape concerne le câblage et l'installation des serveurs. C'est grâce à un réseau de câbles que les ordinateurs seront reliés aux serveurs. Deux options s'offrent à vous selon qu'il s'agit d'un bâtiment neuf ou d'un bâtiment ancien. La première option consiste à encastrer les câbles à l'intérieur des murs et la seconde, à faire recours aux faux-plafonds, aux planchers, ou aux bornes Wi-Fi.

La troisième étape consiste à installer les commutateurs réseau et à paramétrer les logiciels permettant de faire fonctionner les serveurs. Les commutateurs servent à assurer la connexion entre les ordinateurs et les périphériques. La taille de l'installation, les serveurs et les périphériques sont les critères qui déterminent le nombre de commutateurs à installer.

L'étape suivante consiste en l'attribution des adresses IP à chaque poste. Cette formalité facilite l'identification des différents ordinateurs et imprimantes. Elle est relative à la configuration des process de sécurité et des droits d'accès. Car le choix des commutateurs intelligents implique la prise en compte du volet sécuritaire afin de protéger vos machines d'éventuelles intrusions.

L'accessibilité aux serveurs

La configuration des droits d'accès peut être restreinte à un nombre de personnes triées sur le volet. Il s'agit généralement des personnes dignes de confiance. Ce sont les seules personnes autorisées à accéder à la totalité des données de l'entreprise.

Cette configuration permet d'indiquer aux serveurs les ordinateurs qui sont autorisés à se connecter et à accéder à un certain type d'information. On parle alors d'un niveau d'accès associé à chaque catégorie d'utilisateurs. En général, il existe un serveur dédié à chaque département. C'est sur ce dernier que se connectent les personnes qui y travaillent.

Les serveurs informatiques qui ressemblent aux unités centrales sont généralement très esthétiques. Leur installation peut se faire partout dans le lieu de travail, à condition qu'ils soient alimentés et connectés au réseau. Dans le cas contraire, l'installation des serveurs et des commutateurs réseau doit se faire dans une baie de brassage.

Les critères de choix d'une baie de brassage

Deux éléments sont importants dans le choix d'un emplacement pouvant être utilisé comme baie de brassage. Il s'agit entre autres de la profondeur et de la hauteur de cette pièce. En outre, sa capacité à pouvoir accueillir tout le matériel destiné à y être entreposé est aussi un élément important.

S'agissant de la profondeur, la taille des équipements et la surface utilisable sont les deux critères que vous devez prendre en compte, ainsi que l'emplacement des montants.

Comme pour la profondeur, deux éléments importants déterminent la hauteur de la baie de brassage. Une prévision de 40 % doit en effet être effectuée sur la hauteur globale des équipements à installer. L'autre élément à prendre en compte c'est les câbles réseau et leur disposition dans la baie de brassage.

Présentation, maintenance et aération d'une baie de brassage

La centrale d'alarme, le système de télécommunications et l'enregistreur de vidéosurveillance sont autant d'équipements qui peuvent être entreposés dans la baie de brassage. Son intérieur se présente sous diverses formes : armoires avec ou sans roulettes, coffrets à fixer sur le mur et tout autre rangement sans panneaux et sans portes.

L'installation d'une baie de brassage se fait par des professionnels en télécoms et réseaux. Vous pouvez aussi recourir à une entreprise spécialisée dans ce domaine.

Le matériel informatique n'est pas encadré par une réglementation spécifique. Cependant, des mesures doivent être prises vu la quantité de chaleur produite par ces équipements. La mise en place d'un système d'aération ou de refroidissement est une nécessité pour éviter les éventuels risques d'incendie. En cas de sinistre, l'entretien du matériel et la mise en place des mesures de refroidissement seront évalués par les assurances.

Les conditions préalables à la mise en place d'un réseau informatique

Pour mettre en place un réseau informatique, vous devez prévoir l'installation d'un branchement au réseau électrique ou le recours aux énergies alternatives. Ces prévisions concernent non seulement les équipements informatiques, mais aussi les appareils de refroidissement. Ces équipements fonctionnent sous une tension de 220 volts.

Les câbles électriques doivent être séparés des câbles informatiques. Utilisez des goulots différents pour distinguer ces câbles. Un changement de serveur implique de sauvegarder les données à nouveau et de procéder à un contrôle de la conformité de la sauvegarde. En outre, assurez-vous que les données sauvegardées seront réexploitées avant la mise hors tension du serveur.

Une autre précaution consiste à éviter les couloirs de grande circulation pour l'installation d'une baie de brassage. Utilisez les chemins de câbles, les serre-câbles, les passe-câbles et les boîtiers pour masquer vos câbles et multiprises en les protégeant.

Quelques astuces pour l'entretien du matériel

L'utilisation fréquente du matériel informatique rend inutile la mise en place de tests de conformité. Mais en cas d'utilisation sporadique ou d'arrêt prolongé, une vérification des connexions s'impose à une fréquence annuelle.

Le dépoussiérage de vos installations et de vos équipements informatiques doit se faire de façon régulière, c'est-à-dire chaque semaine. Il en va de même du système de refroidissement. Les filtres et les ventilo-convecteurs doivent être nettoyés au minimum une fois chaque année.

Les câbles informatiques ont une durée d'utilisation comprise entre 10 et 15 ans. Leur changement ne peut donc intervenir qu'une fois ce délai atteint. En outre, un professionnel chargé de l'entretien du matériel informatique doit effectuer un contrôle de routine sur ces équipements chaque année.

5 bonnes raisons de passer au Softphone

Parmi les grands enjeux de transformation digitale de l'entreprise, on trouve celui de la joignabilité du collaborateur, surtout quand il est amené à travailler à distance. En passant au softphone, vous pourrez libérer la productivité et l'efficacité des équipes en toutes circonstances ! Vous hésitez encore ? Voici 5 bonnes raisons de repenser votre téléphonie d'entreprise.

Gare aux images d'Épinal et aux confusions : la softphonie et les solutions de visioconférences (telles que Microsoft Teams, Zoom ou Google Meet) ne sont pas concurrentes. Elles sont complémentaires ! Derrière le terme générique de Softphone, on trouve une application qui permet de disposer de toutes les fonctionnalités classiques d'un téléphone fixe, sur un ordinateur, une tablette tactile ou un smartphone. Faire converger téléphonie et informatique présentent de nombreux avantages qui dépassent très largement le fait d'émettre et de recevoir des appels.

Travail collaboratif, agendas partagés, visibilité sur la disponibilité en temps réel, joignabilité à distance, messagerie instantanée... Avec un softphone, vous entrez dans une nouvelle ère de la communication. Pour Anthony Lesueur, chef de projet Marketing pour Linkt, la promesse est claire : « *grâce au softphone, votre numéro de téléphone fixe vous suit partout et ouvre la voie à un nomadisme absolu* ». Si cette perspective ne vous suffit pas, il existe bien d'autres raisons qui devraient achever de vous convaincre !

Raison N°1 : Gagner de la place sur l'espace de travail

Les raisons les plus simples sont souvent les meilleures. Depuis le premier confinement, chacun a appris et admis la nécessité d'exercer, au moins ponctuellement, en télétravail. « *Avec un softphone, observe Anthony Lesueur, le téléphonie fixe disparaît du bureau et à la maison, lorsque l'on travaille sur un coin de table, c'est très appréciable !* ». Une réalité qui vaut aussi dans l'entreprise qui, si elle adopte le Flex-office ou organise des rotations des équipes pour des questions de jauge, n'aura plus à se préoccuper de la disponibilité d'un poste fixe sur chaque table.

Raison N°2 : Le Softphone permet de maîtriser les budgets

Moins de téléphones fixes à acquérir, c'est aussi **moins de téléphones fixes à renouveler et à entretenir** ! Alors que la gestion d'un parc de postes fixes représente un coût non négligeable, nombre d'entreprises faisaient le choix d'en prolonger la durée de vie, dégradant d'autant plus l'expérience collaborateur. « *Le gain financier est également lié aux usages du softphone* », précise Anthony Lesueur. En effet, exploitant les technologies de VoIP (Voice on Internet Protocol, qui permet de faire transiter les communications vocales ou multimédia via Internet), **le softphone permet bien souvent de limiter les coûts des communications, notamment vers l'international.**

Raison N°3 : Booster la performance des collaborateurs

Avec le softphone, la richesse fonctionnelle dépasse largement celle du poste physique, d'autant qu'elle s'enrichit au gré des mises à jour de la solution. « *Chaque utilisateur au sein de l'entreprise, pourra résoudre ses problématiques spécifiques et répondre à ses besoins propres, en utilisant les fonctionnalités qui simplifient son quotidien* », explique Anthony Lesueur. C'est le cas par exemple pour tout ce qui concerne la communication interne. **Messagerie instantanée, gestion de présence, création de conférences de groupes, le softphone démultiplie l'efficacité de chacun.**

Raison N°4 : Développer la dimension collaborative

Parce que le softphone propose une expérience homogène et ergonomique à chaque collaborateur dans l'entreprise, il agit comme un exhausteur de collaborativité ! La possibilité d'**interagir avec l'ensemble des collègues**, de visualiser leur disponibilité en temps réel, d'échanger en messagerie instantanée ou en visioconférence, de consulter les agendas professionnels, mais aussi de centraliser les informations indispensables à des groupes de travail, s'inscrit dans cette attente formulée par les collaborateurs. Une attente qui s'est encore renforcée, à la suite de deux confinements successifs !

Raison N°5 : Garantir la continuité de l'activité en toutes circonstances grâce au Softphone

Et si l'on évoquait le confinement justement et son corollaire immédiat : le télétravail ? Voilà encore une excellente raison d'adopter le softphone. « *Le Softphone répond deux fois à l'enjeu de la continuité de l'activité, y compris en télétravail* », explique Anthony Lesueur. D'abord, **le numéro de téléphone de l'entreprise suit le collaborateur où qu'il se trouve**, y compris dans son salon. Mais alors que la connectivité à la maison n'offre pas toujours les mêmes garanties de disponibilité que la connexion de l'entreprise, « *la possibilité d'utiliser le softphone via un smartphone ou via un ordinateur portable en partage de connexion mobile, assure une joignabilité absolue... y compris en cas de panne d'internet et même d'électricité !* ». Difficile de se montrer plus résilient !



MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité



start **MI** *up*

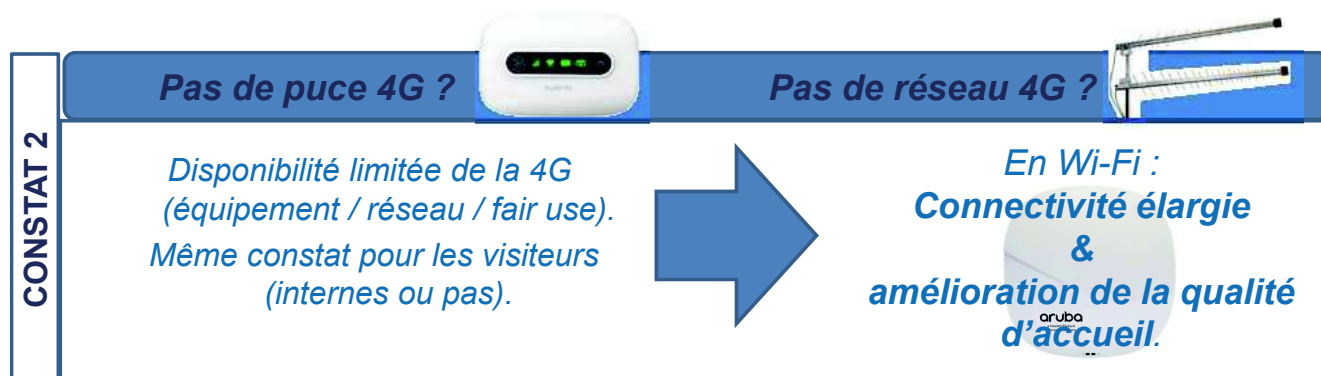
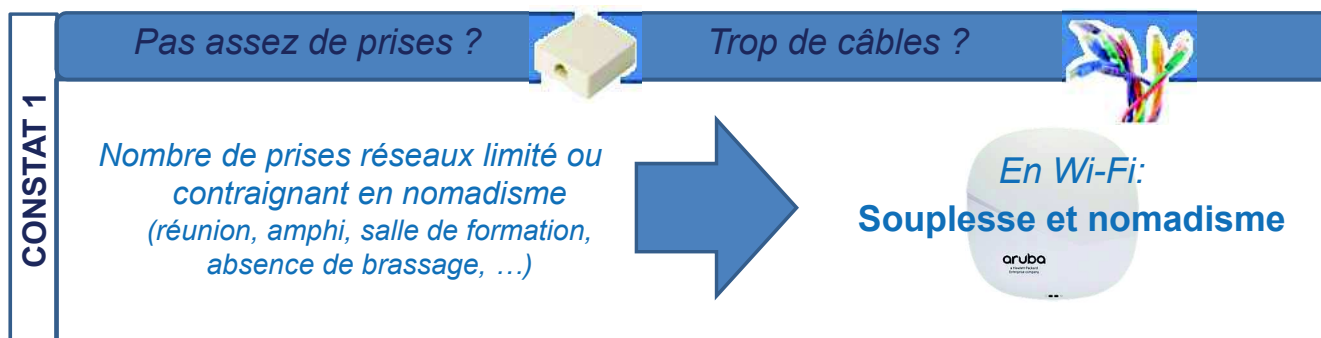
MINISTÈRE DE L'INTÉRIEUR

Mise en place d'une infrastructure Wi-Fi au sein du MI

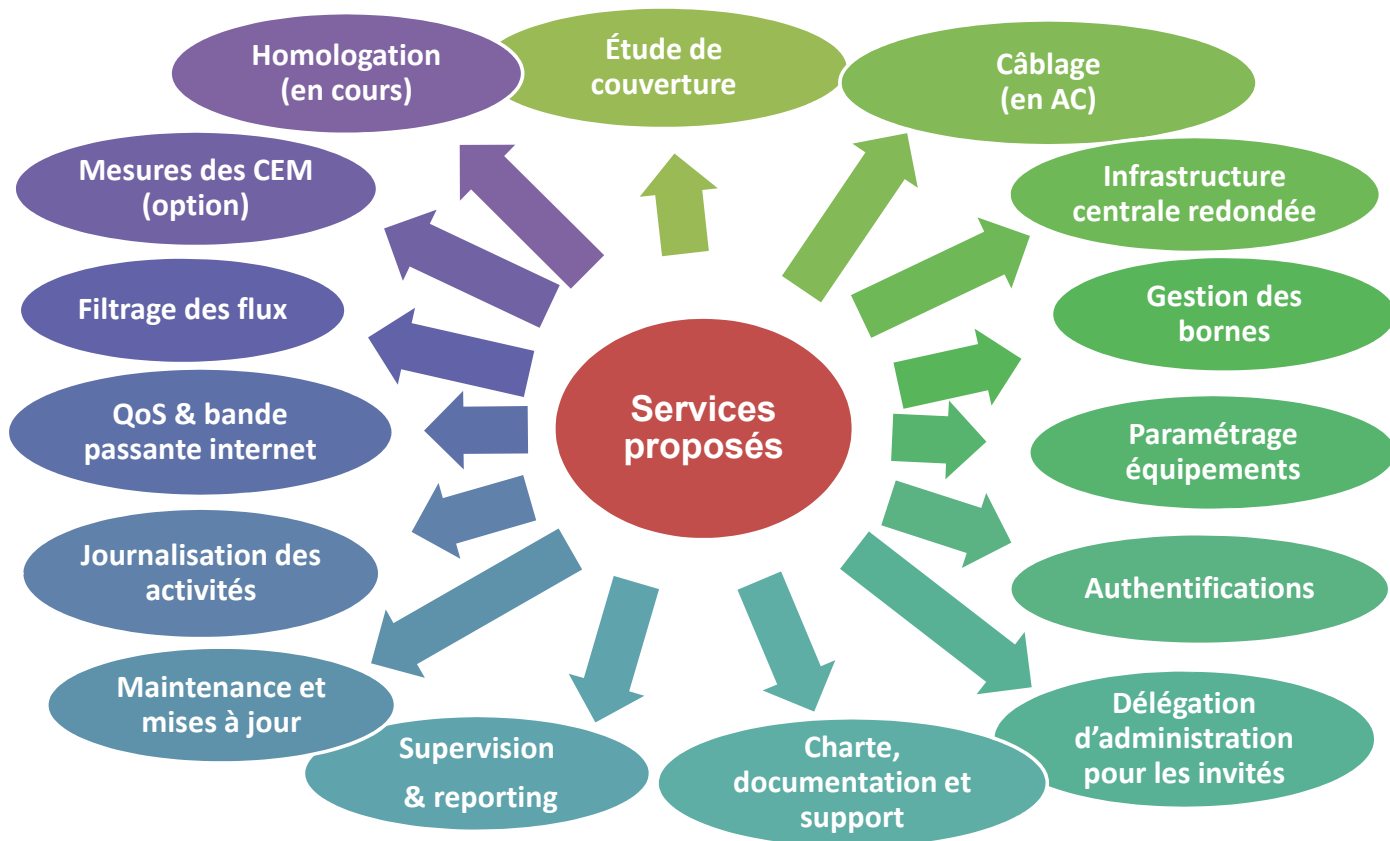
Septembre 2021 (mise à jour numéro 3.7)



Pourquoi le Wi-Fi ?



L'offre STARTMIUP : les services fournis



L'offre STARTMIUP: points forts



- Cloisonnement au réseau filaire (pas d'accès au SI, Internet seul)
- Clé PSK pour les internes + redondance pour haute disponibilité
- Conforme aux recommandations ANSSI (« NP_WiFi_NoteTech »)



- Un pré requis unique : le RIE
- Accès à tous les agents et à leurs invités (agents d'autres entités, prestataires, fournisseurs, ...)



- Une architecture centralisée en datacenter



- Une offre packagée fournissant un ensemble de services
- Une mise en œuvre facilitée en local
- Un accès en tant qu'administrateur délégué pour générer des comptes



- Un accès fédéré, possible depuis tous les sites équipés avec l'offre STARTMIUP (des exclusions de sites restent possibles)



- Les premiers déploiements en AC: Lumière (50 bornes), Beauvau (15 bornes), Lognes (60 bornes), Garance (60 bornes), Nanterre (7 bornes), l'ANTAI (7 bornes), SAELSI (10 bornes), ...



2 modes de connexions
sont identifiées :



INTERNES

- Personnels équipés de **SPAN / CALLMI / NEO / NOEMI** (autres solutions compatibles à venir)
- Connexion: quasi-transparente via une clé secrète PSK (chiffrement et authentification intrinsèques aux solutions)

INVITES

- Visiteurs/personnels avec **équipements propres**
- Service offert : web exclusivement
- Connexion: par ticket d'impression ou par parrainage



Accès visiteurs : génération de tickets en tant qu' « administrateur délégué »

1/ Via un outil sur l'intranet à disposition d'un agent d'accueil du Ministère

- 1) Édition à la demande d'un ticket de connexion
- 2) Depuis son terminal, l'invité se connecte au SSID « WiFi Invites»
- 3) Il est redirigé automatiquement vers un portail captif et saisit l'identifiant et le mot de passe communiqués

Accès invité
Connectez vous au réseau avec votre identifiant et mot de passe

Nom utilisateur :

Mot de passe:

Termes: J'accepte les conditions d'utilisation

Ouverture de session

Besoin d'un compte? [Inscrire](#)

Exemple de ticket :

Détails du compte	
Nom d'utilisateur	71012904
Mot de passe	893513
Activation du compte	lundi, 25 juin 2018, 12:30
Expiration du compte	lundi, 25 juin 2018, 15:00 ou 60 minutes après la première connexion

Au ministère de l'Intérieur, la crise donne « un coup d'accélérateur » aux projets numériques et cyber

Développement du télétravail, sécurisation des communications à distance, attestation numérique de déplacement dérogatoire... La direction du numérique et le ST(SI)2 ont dû réorganiser leurs tâches pour accompagner les personnels du ministère de l'Intérieur et de la gendarmerie dans leurs nouvelles missions, qu'elles soient administratives ou plus opérationnelles. Vincent Niebel, directeur du numérique au ministère de l'Intérieur, et le général Bruno Poirier-Coutansais, chef du ST(SI)2 confirment que la crise liée au Covid-19 a donné un "coup d'accélérateur" à certains projets et en a fait émerger de nouveaux. Olivier de Mazières, Dmisc, estime que la cybersécurité pourrait devenir un "levier de résistance et de résilience" pendant et après la crise.

Brigade numérique de la gendarmerie nationale MaxPPP - David Ademas

"Cette crise va mettre en lumière les investissements à venir pour que le fonctionnement actuel du ministère de l'Intérieur, qui n'est pas complètement optimal dans un contexte de télétravail massif, le devienne", estime Vincent Niebel, dans un entretien à AEF info. Deux mois après la création de la direction du numérique du ministère de l'Intérieur, les 700 personnels affectés en administration centrale à ce service ont dû faire face à un chantier important pour répondre au besoin de protection de l'ensemble des agents du ministère, invités, lorsque cela était possible, à travailler partiellement ou totalement depuis leur domicile.

Le déploiement "plus rapide" de PC sécurisés

"Des outils de télétravail existaient déjà au ministère de l'Intérieur mais le taux d'usage n'était pas à la hauteur de la vague constatée actuellement", explique Vincent Niebel à AEF info. Le premier type d'équipement donnant des capacités complètes de télétravail avec des prises en main sécurisée à distance sur son poste de travail, appelé "Span" était déjà "largement déployé" auprès de plus de 9 000 agents.

La deuxième possibilité de télétravail, appelée "Noemi", avec un PC totalement sécurisé et chiffré permettant de se connecter à l'environnement numérique du ministère de l'Intérieur via un VPN depuis n'importe quelle connexion internet, était "dans sa phase de lancement" et limitée à "quelques dizaines de postes" au début de la crise. "Au premier trimestre 2020, nous voulions initialement tester ce dispositif sur quelques centaines de personnels. Là, ce sont près de 1 500 agents qui en bénéficient" partout sur le territoire, après une formation, détaille Vincent Niebel. "Cette stratégie de dotation et de remplacement de postes de travail fixe a connu un coup d'accélérateur en raison du besoin contextuel de télétravail. La crise a permis de faire démarrer plus rapidement ce projet", se félicite-t-il.

Pour les autres agents non concernés par ces deux possibilités, notamment les personnels non administratifs, "la capacité d'accéder à distance à leur messagerie professionnelle a été généralisée". Au total, "près de 30 000 comptes supplémentaires d'accès distant via un certificat ont été activés, portant à 35 000 le nombre d'agents bénéficiant de cette possibilité".

"Aucune concession" sur la sécurité des outils

"Nous n'avons fait aucune concession sur la sécurité dans le cadre du télétravail", promet Vincent Niebel. Par exemple, l'outil d'accès à distance aux mails se fait par un certificat qui permet d'authentifier la personne, et non pas avec un simple mot de passe. Pour le reste, le niveau élevé de sécurité reste identique à celui d'ordinaire. Toutefois, "le niveau d'attention a été relevé d'un cran et nous en rendons compte quotidiennement".

Par exemple, "la messagerie fait l'objet d'une veille renforcée quotidienne, car comme d'autres structures, les entreprises par exemple, des tentatives de phishing ou de messages comprenant des pièces jointes douteuses nous parviennent". Le service du haut fonctionnaire de défense exploite de façon "encore plus attentive toutes les traces, mêmes faibles, dans notre centre d'analyse et de sécurité".

La cyber, "levier de résistance et de résilience"

"Tous les sujets qui touchent à la cyber vont être des leviers d'abord de résistance face aux attaques et ensuite de résilience", estime Olivier de Mazières. Pour le délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces au ministère de l'Intérieur, "les Jeux olympiques de Paris 2024, qui constituent l'un des objectifs du contrat de filière signé fin janvier et dont le suivi reste une priorité, pourront être la vitrine d'une attractivité retrouvée et le véritable symbole de la résilience du pays".

"Cette crise doit aussi être une opportunité pour pouvoir accélérer et apporter des réponses sur des points de faiblesse identifiés ou confirmés pendant cette période. C'est l'objet de l'inventaire que l'on est en train de faire", déclare le préfet. "Nous sommes en train de dresser le bilan des priorités à fixer pour la sortie de crise, pour savoir quels seront les besoins prioritaires des services et des industries dans les semaines à venir, que ce soit en termes de protection, de fonctionnement, de matériel critique ou de ruptures éventuelles." Cette liste de besoins devra permettre d'activer une sorte de "plan de relance" auquel travaille le ministère de l'Économie et des Finances. Ce plan ne sera pas envisagé avant le mois de septembre 2020, précise Bruno Le Maire sur LCI, mercredi 29 avril 2020.

Pour garantir aux personnels un télétravail sécurisé, le ST(SI)2 a dû également s'assurer de la continuité du service sur les data centers. "Depuis début mars, les modalités de fonctionnement ont été adaptées pour que les équipes ne se croisent pas afin d'éviter des pertes de compétences", indique le général.

80 % de la Dnum à distance

Le télétravail est devenu une réalité pour les personnels de la Dnum concernés "à plus de 80 %" et équipés pour ce faire, des administrateurs jusqu'aux développeurs en passant par les intégrateurs, détaille Vincent Niebel. "Une cinquantaine de personnels de la Dnum travaille encore sur site." Ils assurent la supervision en temps réel de l'ensemble de l'activité, un support de proximité pour les membres de la cellule interministérielle de crise installés à Beauvau, la gestion de l'ensemble des visioconférences sensibles, et des fonctions liées à la production de titres dont l'activité n'a pas cessé, même si la délivrance peut poser des problèmes.

Au final, "le dispositif de pilotage et de fonctionnement s'est bien adapté à la crise", commente Vincent Niebel, qui organise tous les jours des comités de direction de crise réunissant 14 personnels grâce à l'outil interne de visioconférence.

"renforcer les Outils collaboratifs"

La communication à distance est une problématique qui a occupé les techniciens de la gendarmerie et de la Dnum. Les personnels du ST(SI)2 ont œuvré au déploiement d'un système d'audioconférence sur 4 000 sites, souvent également équipés de systèmes de visioconférence. Le DGGN peut ainsi transmettre ses directives et répondre aux questions des commandants de compagnie. Ces audioconférences rassemblent parfois jusqu'à 600 personnels.

La Dnum s'est, elle, attachée à développer un système de visioconférences, de fonctions collaboratives, de partages documentaires, notamment au profit de la cellule interministérielle de crise qui représente "une part importante" de son activité, souligne Vincent Niebel. "Ses moyens de communication avec les territoires – principalement avec les préfetures, les directions départementales interministérielles, et les ARS — ont été renforcés", notamment pour permettre aux hautes autorités d'échanger via un système sécurisé.

En sortie de crise, "nous devons renforcer les outils collaboratifs", anticipe Vincent Niebel. "Le niveau de sécurité et de confiance dans les offres dans le cloud public peut être sujet à caution, notamment concernant les produits de visioconférence. Cette crise révèle la nécessité de travailler, comme nous le faisons déjà en interministériel, sur certains services pour améliorer notre souveraineté numérique, au moins au niveau européen, pour s'assurer qu'en situation de crise comme celle que nous connaissons, nous puissions disposer de services sûrs sur lesquels s'appuyer.

Source : <https://www.aefinfo.fr/depeche/626871-au-ministere-de-linterieur-la-crise-donne-un-coup-d-accelerateur-aux-projets-numeriques-et-cyber>

AO7 Informations générales et documents contractuels

Publication : 29 juillet 2022. Mis à jour : 1 août 2022

Résumé synthétique

L'accord-cadre AO6 a pour objet la fourniture de prestations de téléphonie fixe (accès, communications et services de suivi des factures) en métropole et dans les DROM.

Cet accord-cadre, sans marché subséquent, vient en remplacement de l'AO6.

En métropole, il s'adresse à l'ensemble des entités du MI mais également aux DDI et aux établissements publics sous sa tutelle.

Dans les DROM, il s'adresse à l'ensemble des entités du MI mais également au ministère des finances (Douanes et SCL), au ministère : des affaires sociales (ARS) et aux établissements publics sous la tutelle du MI.

Il comporte 6 lots :

Lot 1 : accès DROM

Fourniture des accès téléphoniques des sites des départements et régions d'Outre-mer, des îles de Saint-Martin et Saint-Barthélemy, et acheminement de l'ensemble des communications téléphoniques entrantes et sortantes de type non présélectionnable.

Notifié le 05/05/2022 à l'opérateur OBS

- Ce lot à été notifié à l'opérateur OBS par la DNUM du ministère de l'intérieur le 05/05/2022
- N° CHORUS : 1300175784

Lot 2 : communications DROM

Acheminement des communications téléphoniques sortantes de type présélectionnable des sites des départements et régions d'Outre-mer et des îles de Saint-Martin et Saint-Barthélemy.

Notifié le 05/05/2022 à l'opérateur OBS

- Ce lot à été notifié à l'opérateur OBS par la DNUM du ministère de l'intérieur le 05/05/2022
- N° CHORUS : 1300175802

Lot 3 : Métropole et DROM ; analyse de trafic s'appuyant sur les données des PABX et analyse des données de facturation fournies par les titulaires des lots 1 à 6.

Fourniture d'une solution de collecte et d'analyse du trafic téléphonique s'appuyant sur les données issues des commutateurs de l'administration et d'une solution de gestion des dépenses téléphoniques s'appuyant sur les données de facturation opérateurs en France métropolitaine, dans les DROM et sur les îles de Saint-Martin et Saint-Barthélemy.

Notifié le 05/05/2022 à la société SAASWEDO

- Ce lot à été notifié à l'opérateur SFR par la DSIC du ministère de l'intérieur le 05/05/2022
- N° CHORUS : 1300175745

Lot 4 : Métropole ; accès T2 "standards" et communications et accès tronc IP et communications

- Fourniture d'accès téléphoniques type accès primaire (T2) en France métropolitaine et acheminement des communications téléphoniques associées, à l'exclusion des accès inclus dans le périmètre du lot 6 :
- Fourniture de troncs de collecte IP en France métropolitaine et acheminement des communications téléphoniques associées.

Notifié le 01/07/2022 à l'opérateur SFR

- Ce lot à été notifié à l'opérateur SFR par la DNUM du ministère de l'intérieur le 01/07/2022
- N° CHORUS : 1300176522

Lot 5 : Métropole ; accès T0 et lignes analogiques "standards" et communications

Fourniture d'accès téléphoniques de type accès de base (T0) et de type ligne analogique, en France métropolitaine et acheminement des communications téléphoniques associées, à l'exclusion des accès inclus dans le périmètre du lot 6 :

Notifié le 01/07/2022 à l'opérateur Orange

- Ce lot à été notifié à l'opérateur OBS par la DNUM du ministère de l'intérieur le 01/07/2022
- N° CHORUS : 1300176505

Lot 6 : Métropole ; accès T2, T0 et lignes analogiques "sensibles" et communications

Fourniture d'accès téléphoniques sensibles ou spécifiques, en France métropolitaine et acheminement des communications téléphoniques associées :

Notifié le 01/07/2022 à l'opérateur Orange

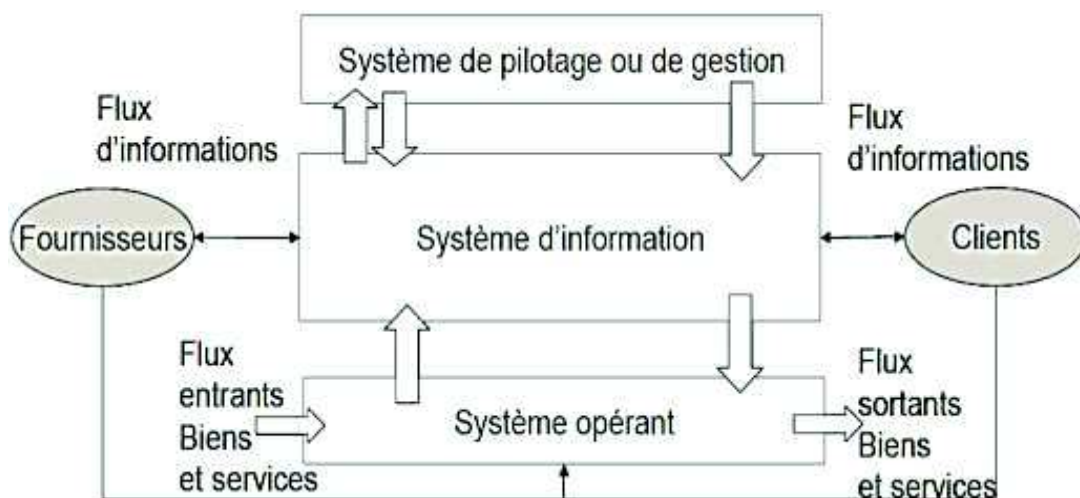
- Ce lot à été notifié à l'opérateur OBS par la DNUM du ministère de l'intérieur le 01/07/2022
- N° CHORUS : 1300176524

Durée du marché :

Pour chacun des lots, le marché est conclu pour une période de 5 ans à compter de la date de notification.

DEUXIEME CHAPITRE - LA CONDUITE DU PROCESSUS DES PROJETS INFORMATIQUES

L'administration d'un projet informatique en mutation requiert un ensemble d'opérations impliquant des exécutions fortuites. C'est pourquoi l'IPMA précise que « *le conduite de projet consiste à planifier, organiser, suivre et maîtriser tous les aspects d'un projet, ainsi que la motivation de tous ceux qui sont impliqués dans le projet, de façon à atteindre les objectifs de façon sûre et dans les critères définis de coûts, délais et performance* ».



II.1. LES ACTIVITÉS DE GESTION DE PROJET

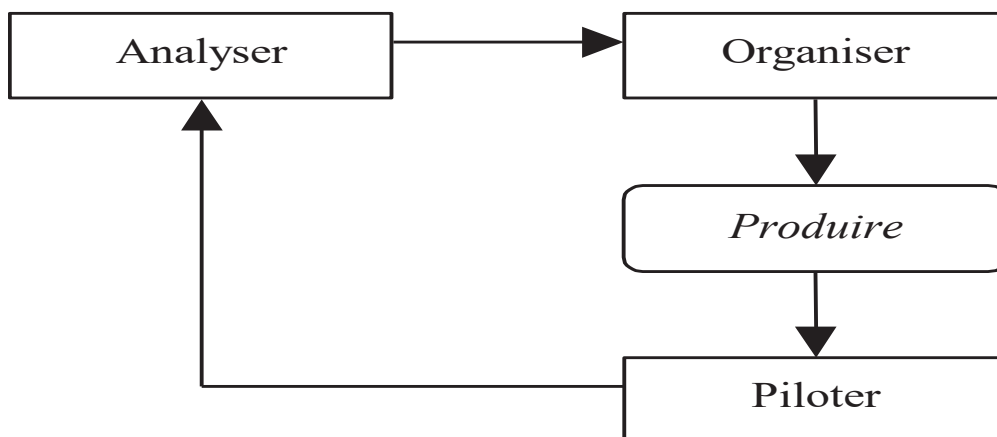
Pour le PMBOK, la gestion de projet est « *l'application de connaissances, de compétences, d'outils et de méthodes aux activités d'un projet afin de répondre à ses besoins* ». Il convient toutefois de distinguer deux catégories d'activités dans un projet :

- **les activités de production** : sont celles qui sont nécessaires pour réaliser le produit ou service visé par l'objectif du projet ;
- **les activités de gestion de projet** : sont celles qui consistent à planifier le travail, l'organiser et suivre l'avancement des activités de production.

Le champ de la conduite de projets informatiques est calé sur les trois aspects représentés par le triangle Projet. Ainsi :

- *Le délai* donne lieu à une *gestion du temps* dont le rôle est de définir le parcours et de le jalonner, d'établir des calendriers et de maîtriser la consommation de l'enveloppe temps.
- *Les moyens affectés* constituent le *budget du projet*, qui est transformé en travail, locaux, matériel, temps machine, déplacement... Cette transformation nécessite une *gestion des ressources* portant sur les ressources humaines et les moyens matériels.
- *L'objectif du projet* doit à son terme être concrétisé par une ou plusieurs fournitures. Cela implique une *gestion de la production*, qui a pour but de suivre et diriger l'avancement vers l'objectif tout au long du projet. On parle parfois de «*faire converger le projet*» : cela signifie qu'il faut sans cesse s'assurer que l'on se rapproche du but et que l'on ne part pas dans des directions remettant en cause un avancement consolidé.

On peut décomposer l'activité de la conduite des projets informatiques en trois activités principales autour de la production proprement dite :



Les activités de gestion de projet

- ***Analyser*** : consiste à déterminer le chemin que l'on va emprunter pour avancer vers l'objectif. Pour cela, on étudie les caractéristiques du projet, son contexte, les risques qui le menacent et l'état de son avancement. Cela conduit à un découpage du projet en actions à entreprendre et à une estimation de l'effort nécessaire. La maille de cette analyse varie selon le moment du projet auquel on se place.

- **Organiser** : signifie repérer les contraintes d'enchaînement entre les tâches afin de les ordonnancer. Cela permet d'établir un calendrier. L'organisation recouvre aussi la constitution d'une équipe, c'est-à-dire des personnes qui sont affectées et imputées au projet, en déterminant les bons profils. Les relations avec tous les partenaires nécessaires sont également prises en compte. Dès que la charge est importante, on répartit le travail entre plusieurs personnes, voire plusieurs équipes, ce qui conduit à mettre en place des moyens de partage d'informations pour éviter les incohérences.
- **Produire** : consiste à assurer les actions diverses (*cultures, fabrications, etc.*) qui concourent à fournir sur le marché commercial certains biens ou services.
- **Piloter** : comprend le suivi de l'avancement du projet, en quantité et en qualité, ainsi que l'analyse et le traitement des écarts avec ce qui était prévu, les orientations et les décisions à prendre ou à faire prendre. Le pilotage inclut également le management de l'équipe et la gestion des conflits.

Pour la norme ISO10006: 2003, les activités de gestion de projet sont organisées en processus, et réparties en quatre familles :

- **La première famille** ne comprend qu'un seul processus, appelé processus stratégique, qui regroupe les activités relevant de la responsabilité de la direction de l'entreprise, telle que la nomination des chefs de projet.
- **La deuxième famille** comprend des processus qui touchent à la gestion des ressources, en particulier le personnel.
- **La troisième famille** structure les activités de gestion de projet orientées vers la réalisation du produit, c'est-à-dire la production du bien ou service visé par l'objectif. Elle comprend la coordination des activités, la maîtrise des tâches de production, la maîtrise des délais et des coûts, la gestion de la communication, la maîtrise des risques et celle des achats pour le projet.
- **La quatrième famille** de processus réunit les activités de gestion de projet, qui visent l'amélioration, c'est-à-dire le management des connaissances issues des projets achevés.

IV.2.2. LES TECHNIQUES D'ESTIMATION DE PROJETS INFORMATIQUES.

L'estimation des projets informatiques est l'une des plus importantes activités du développement de logiciels. La planification rigoureuse et le pilotage du projet ne sont pas envisageables en absence d'une estimation sérieuse et fiable. En règle générale, notre industrie du logiciel ne sait pas estimer correctement les projets et n'utilise pas convenablement les estimations. Nous souffrons de ces conséquences et nous devons focaliser nos efforts sur l'amélioration de la situation. La sous-estimation d'un projet entraîne :

- Un sous-effectif, provoquant la surchauffe de l'équipe ;
- Une sous-appréciation de la charge d'assurance qualité, avec le risque de livrables de médiocre qualité ;
- L'établissement d'un planning trop serré, qui dégradera votre crédibilité, lorsque ces délais présomptueux sont largement dépassés.

Pour ceux qui pensent éviter cette situation en gonflant l'estimation, la surestimation d'un projet peut s'avérer aussi néfaste pour l'Organisme. Si vous accordez à un projet plus de ressources que nécessaires sans contrôler l'utilisation de ces ressources, le projet :

- Coûtera beaucoup plus cher (en grevant le bilan du projet) ;
- Durera plus longtemps que nécessaire (en manquant les opportunités ciblées) ;
- Diffèrera la disponibilité de vos ressources pour le prochain projet.

IV.2.2.1. ESTIMATION DE CHARGES DE PROJETS INFORMATIQUES

L'estimation d'un projet informatique comprend quatre étapes :

- Estimer la taille du produit à développer. Celle-ci se mesure généralement en nombre d'instructions (lignes de code) ou en points de fonction, mais il existe d'autres unités de mesure possibles. Une comparaison des avantages et des inconvénients de chacune de ces mesures est abordée dans les références bibliographiques données en fin de l'article.
- Estimer la charge en mois hommes ou en jours hommes ;
- Construire le calendrier du planning ;
- Estimer le coût du projet en monnaie locale ;

Source : Cours de méthodes de conduite des projets informatiques – YENDE RAPHAEL Grevisse

ComU, l'outil de visioconférence du ministère de l'Intérieur

L'application de Communication Unifiée du ministère de l'Intérieur (ComU) permet, à travers un moyen numérique, de voir et dialoguer avec des participants éloignés, tout en rendant possible le partage de documents.

Avec ComU, vous pouvez joindre les agents d'**autres ministères** grâce à des **ponts interministériels**. Les **partenaires extérieurs** sont quant à eux joignables via des **ponts nationaux**.

L'outil intègre aussi la possibilité d'**enregistrer les débats** et de **sécuriser les réunions**. Il suffit d'en faire la demande au pôle de visioconférence.

Tous les agents du ministère peuvent utiliser ComU pour rejoindre une visioconférence.

L'application ComU est accessible depuis :

- NOEMI ou poste individuel
- Une salle de réunion ou un terminal de visioconférence

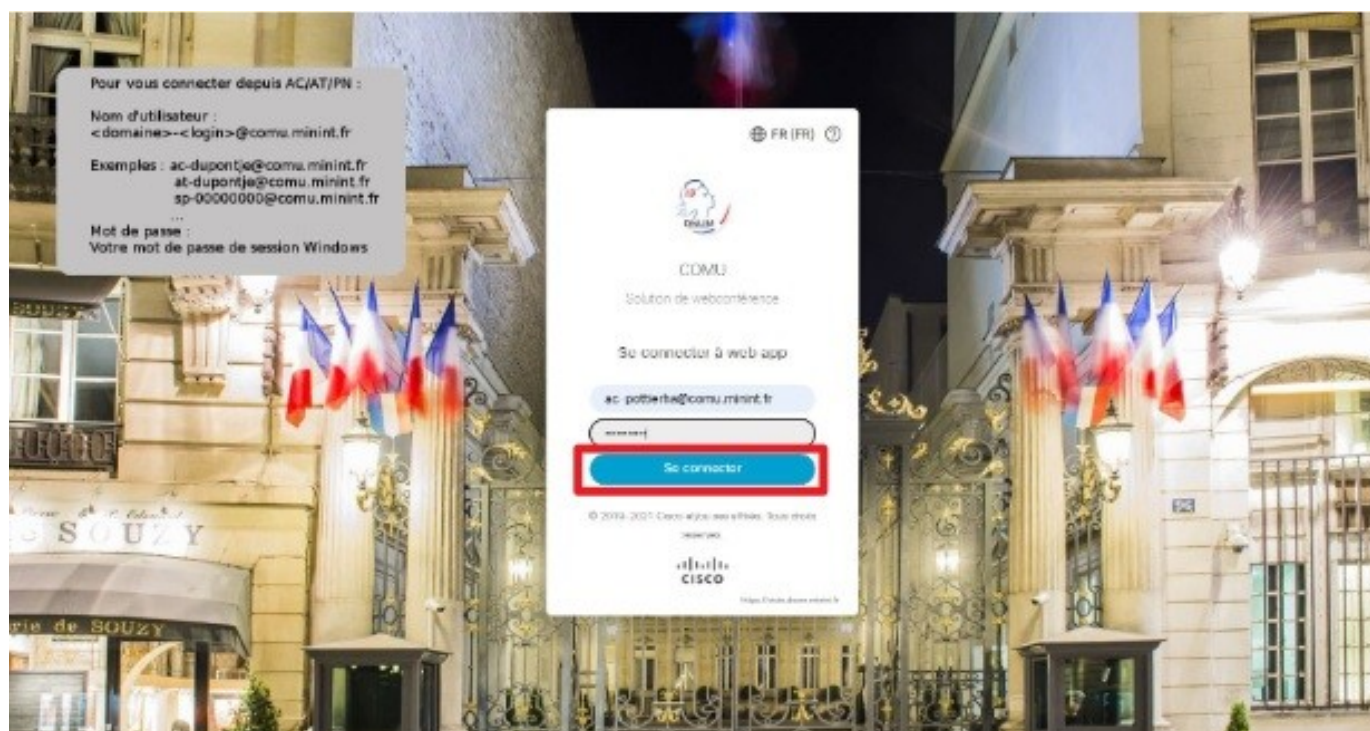
Prérequis

1. Disposer de la dernière version du navigateur Chromium sur son poste de travail. Pour l'installer, adressez-vous à votre service informatique local. La dernière version est disponible sur DNUM Téléchargement.
2. Disposer de vos **identifiant** et **mot de passe de session Windows**

Comment accéder à une conférence sur l'application comU

Cisco Meeting Server web app (web app), communément appelé COMU, est un client basé sur le navigateur Chromium permettant aux utilisateurs de rejoindre les réunions (audio et vidéo).

Lorsque vous êtes invité à une réunion, vous pouvez utiliser les informations qui vous sont envoyées pour rejoindre votre réunion à partir d'un poste de travail du Ministère de l'Intérieur, via un terminal de visioconférence ou en audioconférence.



Source : Document interne, DNUM

La ToIP, une solution de téléphonie d'entreprise à envisager au plus vite !

Si la téléphonie sur IP (ToIP) est à la portée de toutes les entreprises, son adoption doit être étudiée au cas par cas selon la taille de la structure, de l'existant, de ses besoins, etc. Présentation de cette technologie aujourd'hui incontournable.

SIP, téléphones logiciels et visiophonie

SIP (Session Initiation Protocol) est en quelque sorte le standard universel de la ToIP, c'est le protocole qui est utilisé pour gérer les communications. Grâce à lui, les utilisateurs peuvent échanger des données de texte, de voix et de vidéo. En fonction du terminal distant (téléphone, IPBX, etc.) et du type de destination (téléphone fixe, pays étranger, etc.), il adapte les caractéristiques de la communication pour en améliorer la qualité et la fiabilité. Il joue essentiellement sur les codecs audio et vidéo, leviers primordiaux car ils permettent de retranscrire le son et l'image, de comprimer les flux et d'optimiser la bande passante notamment.

Les téléphones logiciels ou « softphones » permettent d'émettre et recevoir des appels depuis son ordinateur en utilisant un micro-casque.

Un employé sédentaire préférera généralement un téléphone matériel tandis qu'un utilisateur nomade appréciera toutes les possibilités de son softphone à mesure qu'il changera de lieu de travail. Cette option évite aussi l'acquisition d'un téléphone matériel. A noter qu'un téléphone logiciel est toujours utile de façon ponctuelle pour profiter d'une visioconférence ou simplement lors de sessions de télétravail.

Et pour les plus technophiles, sachez que Jabber fonctionne avec votre Apple Watch. Mais aussi avec votre montre connectée sous Android.

La Visio(phonie) est quant à elle gérée nativement par la ToIP. Elle permet d'établir un échange vidéo avec son interlocuteur directement depuis son téléphone, aussi simplement qu'un appel. La seule contrainte est que les deux utilisateurs disposent d'un terminal compatible.

Quels sont les avantages du passage à la ToIP ?

Le passage à la ToIP offre de nombreux avantages, notamment une **mobilité** et une **disponibilité** particulièrement appréciables pour les structures disposant d'employés en télétravail ou d'une configuration multi-sites. La « gestion du débordement » accroît elle aussi la **flexibilité** de la structure. De façon concrète, certains départements dans votre société peuvent faire partie d'un groupement d'appels, leur permettant d'intercepter les appels de collègues indisponibles. Lorsqu'une secrétaire est en ligne et doit faire face à un nombre d'appels trop important, un utilisateur peut choisir de faire sonner son terminal ou celui d'un collègue. Avec ce type de solution, les appels ne sont jamais perdus.

Un Serveur Vocal Interactif vous permet de donner une image plus professionnelle à votre société. Il s'agit de la gestion d'un script pour le traitement efficace des appels entrants, la qualification et l'orientation vers le bon interlocuteur.

On observe également une **hausse de la productivité des employés suite à l'adoption des ToIP**. Grâce à cette technologie, les utilisateurs peuvent envoyer des SMS depuis leur ordinateur, créer des boîtes vocales différenciées (en fonction du jour et du mois) ou encore mettre en place une gestion des auto-calls. Cette dernière fonctionnalité permet de passer un appel directement depuis son ordinateur (clic ou raccourci clavier). Un gain de temps considérable pour les employés au téléphone une grande partie de la journée.

Autre avantage important aux yeux des décideurs : la **réduction des coûts de communication**. L'investissement initial est en effet très limité, tout comme le temps de déploiement. Les procédures d'assistance sont de plus relativement simples grâce à un réseau informatique unique mutualisant la Voix et la Data. Les entreprises multi-sites profitent d'une suppression totale des coûts de communication entre les employés dispatchés géographiquement. Pour ne rien gâcher, le prix des appels vers les mobiles et à l'international est moins élevé et les appels nationaux réglés sur une base forfaitaire.

Si la ToIP s'est développée si rapidement ces dernières années, c'est aussi parce qu'elle permet à une entreprise d'homogénéiser ses équipements téléphoniques, de profiter de solutions novatrices sans surcoût et de mettre en conformité ses installations en vue d'accueillir les solutions de demain.

Point sur la terminologie de la téléphonie professionnelle

En termes générique, on parle la plupart du temps d'autocommutateur téléphonique privé ou de standard téléphonique. Pour aller plus loin, voici la signification des principaux termes techniques :

- **PABX** (Private Automatic Branch Exchange) : système utilisé pour raccorder les lignes téléphoniques d'une entreprise au réseau public extérieur géré par les opérateurs
- **IPBX** (Internet Protocol Branch Exchange) : même fonction que le PABX mais tourné vers l'IP, il utilise pour cela le réseau informatique
- **VPBX** (Virtual PBX) : IPBX virtuel et hébergé sur un serveur informatique de l'entreprise
- **VoIP** (Voice over Internet Protocol ou voix sur IP) : technologie de transport de la voix sur un réseau compatible IP
- **ToIP** (Telephony over Internet Protocol ou Téléphonie sur IP) : technologie de transports de la signalisation et des flux voix sur un réseau local
- **Trunk SIP** : service de connectivité pour transporter les communications vocales en IP

En conclusion, la ToIP est un outil technique et un moyen pour une entreprise d'augmenter sa productivité, sa compétitivité et d'étendre sa disponibilité. Les fonctionnalités croissantes offertes par la technologie sont aujourd'hui suffisantes pour franchir le pas. Reste à choisir la solution la plus adaptée en fonction de ses usages et besoins. Il est conseillé de faire appel à un professionnel pour ce type de transition.

Produits numériques partagés

Communiquer, collaborer, dématérialiser

8 produits numériques interministériels collaboratifs

- Ouverts à tous les agents de l'État
- Accessibles aux partenaires externes
- Simples et répondant aux besoins communs
- Utilisables au bureau et en télétravail
- Complémentaires aux environnements numériques ministériels
- Souverains et sécurisés



Suivez les actualités de la direction interministérielle du numérique sur : numerique.gouv.fr

NOEMI

Portable

La solution NOEMI s'adapte à vos besoins et répond aux nouveaux modes de travail en mobilité.

VIP



NOMADISME



TÉLÉTRAVAIL



FORCES OPÉRATIONNELLES



Découvrez également
NoéMI Tiny



Tiny



La solution NOEMI offre aux agents du Ministère de l'Intérieur un ordinateur ultranomade sécurisé. Il est connecté au travers d'un VPN sur l'infrastructure du MI.

ATTENTION : Compte tenu des délais pour obtenir une nouvelle carte agent et du fait de l'augmentation du télétravail, deux versions de NOEMI sont désormais proposées : Sans Carte (SC) ou Diffusion Restreinte (DR). Dès que l'agent récupérera sa carte agent, il basculera automatiquement sur la version DR.

NOEMI SC

- **Authentifications via :**
 - Login Cryhod + MDP n°1
 - Login Windows + MDP n°2
- Permet d'accéder à toutes les applications éligibles au télétravail* **hors applications nécessitant une authentification forte.**

NOEMI DR

Homologué DR



- **Authentifications via**
 - Carte agent
 - Code à 4 chiffres
- Permet d'accéder à toutes les applications éligibles au télétravail*.

*Pour plus d'informations sur les applications éligibles, rendez-vous sur ssi.minint.fr, sections Réseaux de communication sécurisés/ISIS/Espace Services/Outils/Nomadisme : SPAN

Connexion multimodale



ETHERNET
(via réseau MI)



WIFI
(ministère ou personnel)



PARTAGE DE CONNEXION
(via tel. personnel)



CARTE SIM 4G
(via marché Opache 5)

Hors-connexion, il est également possible de travailler sur les documents enregistrés sur le poste.

Au ministère



Package bureautique : 1 ou 2 écrans, souris, clavier



Station d'accueil



NoéMI Portable

En nomadisme

Alimentation



- Une manipulation simple et rapide au Ministère : avec la station d'accueil, **un seul branchement est nécessaire.**

- 1- Alimentation
- 2- Réseau
- 3- Souris et clavier
- 4- Ecran



Références compatibles

Dell Latitude 5310

Ref. UGAP : 2914856 (8Go), 2914860 (16Go)



8Go

HD Intel i3-10110U

13,3 pouces ; 1,22 kg

Windows 10 Pro

256 SSD

Garantie 4 ans retour atelier

Station d'accueil – Réf. UGAP : 2864608

Sacoche – Réf. UGAP : 2864609

Filtre écran – Réf. UGAP : 2864612

Lecteur de carte agent et lecteur 4G intégrés

16Go

HD Intel i5-10210U

Lenovo ThinkPad

Ref. UGAP : 2933081 (X13), 2933080 (L15)



Version X13

16Go

Ryzen 5 Pro 4650U

13 pouces ; 1,29 kg

Windows 10 Pro

512 SSD

Garantie 4 ans sur site J+2

Station d'accueil – Réf. UGAP : 2864608

Sacoche – Réf. UGAP : 2864609

Filtre écran – Réf. UGAP : 2864612

Lecteur de carte à commander à part sur l'UGAP

Version L15

15 pouces ; 1,98 kg

Contactez-nous

Pour commander sur le marché ODICE2 (UGAP) : Marc Cavallero - mcavallero@ugap.fr



Le RIE, un réseau efficace en trois composants, performant et évoluant en trois axes.

Mis en œuvre par le département infrastructures et services opérés (ISO) de la DINUM, le **réseau interministériel de l'État (RIE)** a été conçu pour assurer le support des transmissions de données de l'ensemble des systèmes informatiques constituant le système d'information et de communication de l'Etat. Il est ouvert (et d'usage obligatoire pour les transmissions non protégées et non spécifiques) à **l'ensemble des services de l'État sur le territoire national, DROM et CTOM inclus**. Il ne dessert pas à ce jour les sites à l'étranger tandis que les services du ministère de l'éducation nationale utilisent [Renater](#) et l'interconnexion entre ce réseau et le RIE. De leur côté, les sites non opérationnels du ministère des armées seront progressivement basculés sur RIE entre cette année et 2023, le ministère des armées utilisant déjà le RIE pour certains services dont le télétravail.

Les opérateurs de l'Etat peuvent également interconnecter leurs propres réseaux de transmission de données avec le RIE afin d'obtenir des accès à certains services applicatifs exposés sur le RIE (typiquement, mais pas exclusivement, les applications transverses de type SIRH ou SI Financier, souvent partagées avec le ou les ministères de tutelle). Pour des raisons historiques ou d'opportunité, certaines institutions et certains établissements publics sont directement connectés au RIE par l'intermédiaire de leur ministère de tutelle ou dans le cadre d'un hébergement informatique interministériel (la DILA, le Défenseur des droits, le CSA, l'IGN, les ARS, les SDIS, l'ANTS, les lycées maritimes...) mais cela reste une exception.

On présente souvent le RIE en trois grands composants :

- Le **réseau de collecte** est la partie la plus visible du RIE. Ce réseau dessert aujourd'hui un peu plus de **13 000 sites utilisateurs**, exposant une très grande diversité : de l'abattoir de Saint-Gaudens au site Bercy des ministères économiques et financiers, en passant par le phare de Collioure, la brigade territoriale de Gendarmerie de Loures-Barousse, la préfecture de Privas, la DRAC de Lyon, la DREAL de Nantes... Environ **un million d'utilisateurs internes** utilisent les services du RIE.

Cette partie du réseau recourt pour l'essentiel aux services professionnels des opérateurs nationaux Orange, SFR et, dans une moindre mesure, Bouygues Télécom. Huit niveaux de sécurisation existent, depuis l'accès ADSL simple jusqu'au double accès fibre optique garanti sans point de défaillance unique. Afin de répondre à un besoin de sécurité encore plus élevé, un neuvième niveau est à l'étude, qui proposera un accès avec deux fibres optiques relevant de deux opérateurs différents

Cette partie du réseau a pour mission de collecter (d'où son nom...) les flux des sites utilisateurs jusqu'à l'épine dorsale du RIE.

- **L'épine dorsale** du RIE est composée d'une boucle optique à très haut débit exposant 12 points de présence – les PIB – installés au sein de centres de production informatiques critiques de l'Etat.

Cette épine dorsale est constituée de liens sous-loués à Renater et éclairés par ce dernier, raccordés à des commutateurs de forte puissance propriétés de l'Etat et infogérés par Orange. Le niveau de maîtrise de cette infrastructure est donc très élevé (location des liens à un GIP essentiellement étatique, équipements propriétés de l'Etat, exploitation sous pilotage direct de l'Etat).

Les missions essentielles de l'épine dorsale sont (i) la distribution des flux de collecte sur l'ensemble des centres de production informatiques de l'État et (ii) la résilience de l'interfonctionnement entre ces centres de production informatiques, y compris en situation de crise opérationnelle majeure – par exemple pour compenser la perte de réseaux commerciaux de transmission de données.

- **Les équipements** assurant l'interfonctionnement entre le RIE et les réseaux tiers ainsi que la défense en profondeur du réseau : **PFAI** (plateforme d'accès à internet) et **PFS** (plateforme de services, assurant notamment le cloisonnement interne du réseau). Ces équipements permettent de garantir la sécurité de l'interconnexion des réseaux ministériels entre eux et avec internet bien sûr, mais également avec Renater, avec sTesta (le réseau d'interconnexion pan-européen entre intranets gouvernementaux des 27 pays de l'Union) ou encore les réseaux propres des opérateurs de l'Etat partenaires du RIE.

L'ensemble des composants du réseau fait l'objet d'une supervision 24/7 opérée directement par le pôle Hypervision/Supervision du département ISO depuis son site de Rennes. Cette supervision, associant une équipe de techniciens généralistes (NOC : *Network Operation Center*) et une équipe plus axées sur les sujets de sécurité (SOC (*Security Operation Center*)), apporte son expertise à l'analyse et la résolution des dysfonctionnements constatés quotidiennement sur le réseau. Ce pôle traite ainsi plusieurs dizaines d'incidents chaque jour, heureusement sans gravité la plupart du temps, et des attaques fréquentes, également essentiellement sans impact grâce aux contre-mesures automatiques et, si nécessaires, manuelles mises en œuvre par le SOC.

Parmi les autres chiffres clés intéressants : **6000 changements / an** environ sur la partie collecte (création de sites, déménagements, augmentations de débit, ajout de canaux spécifiques type voix/vidéo ou de communautés ministérielles), **plus de 200 réseaux virtuels** assurant le cloisonnement entre les différents réseaux ministériels, un trafic de plus de **12 Gbps aux heures de pointe au niveau de l'interfonctionnement avec internet...**

Le réseau fait actuellement l'objet de trois programmes majeurs d'évolution :

- Le **programme Résilience RIE** vise à **améliorer la résilience du réseau** sur ces trois principaux composants dans la perspective de l'accueil, à l'horizon 2022, de services reprenant les actuels services offerts par le réseau Rimbaud, réseau durci spécifiquement dédié à la continuité de l'action gouvernementale et appelé à disparaître en raison de son obsolescence technologique :
 - Au niveau collecte, en ajoutant un neuvième niveau de sécurisation (H, voir ci-dessus)
 - Au niveau de l'épine dorsale, en construisant une seconde boucle optique avec des liens loués à un autre opérateur (sans doute la SNCF)
 - Au niveau de l'interfonctionnement avec internet, avec la conception d'une nouvelle PFAI dédiée aux flux critiques (typiquement associés à la gestion de crise)

- Le **programme RIE 2.0** vise à **développer et rationaliser les services offerts par le réseau**, là également avec une déclinaison sur les trois composants :
 - Au niveau collecte en formalisant le recours à de nouvelles technologies, notamment la 4G/5G et l'appui sur des services de type FTTH (dans une optique bas coût et de remplacement à terme des accès cuivre)
 - Au niveau de l'épine dorsale avec la rationalisation de la carte des PIB afin de l'aligner sur le plan TCI de la DINUM (cartographie des centres de production informatiques pérennes de l'Etat) et la simplification de l'interface entre l'épine dorsale et le réseau de collecte (passage de 12 à une seule plaque de collecte).
 - Au niveau de l'interfonctionnement avec les réseaux tiers avec la mise en place d'appairages directs avec certains acteurs du cloud permettant de décharger les liens de transit internet – sans impact sur le niveau de sécurité – de certains flux.

- Le **programme RIE THD**, inscrit dans la perspective du plan de relance, vise à améliorer le confort des utilisateurs en **augmentant les débits disponibles**. Il est, lui également, décliné sur trois axes :
 - Au niveau de la collecte au travers de l'initiative SNAP 1, dotée de 10 M€, visant à accompagner les ministères bénéficiaires dans le passage massif à la fibre optique et l'augmentation des débits bruts sur les sites utilisateurs,
 - Au niveau de l'épine dorsale, avec le passage de 10 à 100 Gbps des capacités des liens Renater (auquel s'ajoute la mise en place des liens de la seconde boucle optique, dès le départ à 100 Gbps)
 - Au niveau de l'interfonctionnement avec les réseaux tiers, avec l'augmentation progressive des débits des liens de transit : dans ce domaine, le réseau est ainsi déjà passé, en quelques mois, d'une capacité de 16 (automne 2019) à 22 Gbps (hiver 2021) de débit brut).

RIE V2 : Profils et Débits des accès

Collecte IP VPN Classique				Raccordement N2	
OBS	SFR	SFR	SFR	OBS	SFR
Lot 1	Lot 2	Lot 3	Lot 4	Lot 5	Lot 6
Service de collecte IP VPN Premium Fibre	Service de collecte IP VPN Standard Fibre	Service de collecte IP VPN Cuivre	Service de collecte IP VPN Economique	Service Ethernet Premium	Service Ethernet Standard
2xFO 10M	FO 10M	SDSL 2M	FTTx	Ethernet 2xFO 100M	Ethernet 2xFO 250M
2xFO 20M	FO 20M	SDSL 4M	VDSL	Ethernet 2xFO 200M	Ethernet FO 500M
2xFO 50M	FO 50M	SDSL 8M	ADSL	Ethernet 2xFO 500M	Ethernet 2xFO 500M
2xFO 100M	FO 100M	2xSDSL 2M	Accès 4G/5G	Ethernet 2xFO 1G	Ethernet FO 1G
2xFO 200M	FO 200 M	2xSDSL 4M		Ethernet 2xFO 2G	Ethernet 2xFO 1G
2xFO 500M	FO 10M + FTTx ou accès 4G/5G	2xSDSL 8M		Ethernet 2xFO 5G	Ethernet FO 2G
2xFO 1G	FO 20M + FTTx ou accès 4G/5G	SDSL 2M + FTTx ou accès 4G/5G		Ethernet 2xFO 10G	Ethernet 2xFO 5G
	FO 50M + FTTx ou accès 4G/5G	SDSL 4M + FTTx ou accès 4G/5G		Ethernet 2xFO 20G	Ethernet FO 10G
	FO 100M + FTTx ou accès 4G/5G	SDSL 8M + FTTx ou accès 4G/5G		Ethernet 2xFO 50G	Ethernet FO 20G
	FO 200M + FTTx ou accès 4G/5G			Ethernet 2xFO 100G	Ethernet FO 50G
					Ethernet FO 100G

Source : Document interne ministère de la transformation et de la fonction publiques

Contrôle d'accès RFID : qu'est-ce que c'est et comment ça marche ?

Le système de contrôle d'accès RFID permet de déterminer qui entre ou sort de locaux spécifiques à un moment donné. Il comprend un système automatisé qui identifie un individu, authentifie ses coordonnées et permet l'accès après vérification.

Le système est conçu pour permettre uniquement à des personnes spécifiques d'accéder à un bâtiment. Ces personnes doivent posséder un Carte RFID, porte-clés RFID, Bracelet RFID, ou toute autre forme de Étiquette RFID contenant leurs détails de vérification.

Si cela semble déroutant, alors ne vous inquiétez pas ! Cet article propose un guide complet sur le fonctionnement des systèmes de contrôle d'accès RFID.

Qu'est-ce qu'un système de contrôle d'accès RFID ?

RFID est un acronyme pour Radio Frequency Identification. Il s'agit d'un système qui utilise des ondes radio pour transmettre des informations.

Un système RFID complet doit avoir un lecteur et une étiquette. L'étiquette doit de préférence être accessible en écriture et en lecture pour que vous puissiez écrire des détails uniques sur une personne en particulier.

De plus, l'attribut écriture/lecture vous permet d'utiliser une seule balise pour différentes personnes à différents moments. Par exemple, lorsqu'un employé démissionne, vous pouvez facilement effacer ses données et écrire de nouvelles données pour un nouvel employé.

Pour qu'un système d'accès RFID fonctionne de manière optimale, il doit avoir tous les composants énumérés ci-dessous :

Composants d'un système de contrôle d'accès RFID

- **Le serveur.** Ce composant contrôle la liste blanche (une liste de toutes les personnes autorisées à accéder à un local donné). Le système est contrôlé par la direction en saisissant/enregistrant les identifiants de tous les visiteurs attendus.
- **Expérience.** Il s'agit de détails spécifiques qu'une organisation choisit d'utiliser pour l'identification des visiteurs/employés. Il peut s'agir de n'importe quoi allant des NIP uniques, des numéros de carte d'identité et des codes uniques, entre autres. Il n'y a pas de norme pour les informations d'identification et les données à utiliser sont uniquement déterminées par la direction.
- **Tags RFID.** Ce composant est l'endroit où les informations d'identification sont stockées. Les détails écrits sur les balises doivent correspondre exactement aux détails de la liste blanche. Toute erreur de copie des données entraînera le rejet du tag par les lecteurs. L'étiquette peut être attachée à n'importe quoi, y compris des cartes, des porte-clés, des bracelets et des bracelets.
- **Lecteur RFID.** Un lecteur RFID doit être placé stratégiquement pour scanner les étiquettes RFID. Si les informations stockées dans l'étiquette correspondent à celles de la base de données du système, l'utilisateur étiqueté sera autorisé à accéder.
- **Contrôleur.** Ce composant compare les données capturées par le lecteur RFID avec les informations stockées dans la liste blanche. Il envoie un signal à la serrure de la porte pour qu'elle s'ouvre uniquement si les informations d'identification correspondent.
- **Verrou.** Le système de verrouillage de porte RFID est automatisé et entièrement dépendant du contrôleur. Le panneau de commande enverra soit des signaux d'ouverture/fermeture. À la réception de ces signaux, la porte s'ouvrira ou restera fermée, selon le type de signal reçu.

Bien que cela puisse sembler un long processus, il est rapide comme l'éclair ! L'ensemble du processus d'identification prend quelques secondes !

Comment fonctionne le contrôle d'accès RFID

La fonctionnalité du système de contrôle d'accès RFID peut être simplifiée en 2 étapes simples :

- Présentation des données
- Autorisation/Authentification des données

Présentation des données

Il s'agit de la phase initiale du contrôle d'accès. Cela nécessite que les données soient présentées au lecteur RFID pour analyse.

Les données peuvent être présentées sous diverses formes selon les besoins et les préférences de la direction. Cependant, les données codées doivent être uniques à des employés spécifiques. La duplication des données entraînera des erreurs pouvant retarder l'admission.

La présentation des données suit les étapes suivantes :

- **Mise à jour des données sur le système de contrôle.** Le système de contrôle est l'élément décisionnel clé d'un système de contrôle d'accès RFID. C'est la mémoire de l'organisation. Il stocke toutes les données nécessaires à l'admission dans les locaux. La direction doit le mettre à jour avec les identifiants des visiteurs attendus.
- **Rédaction d'étiquettes RFID.** Une fois que la direction a déterminé la combinaison de données à utiliser dans le système de contrôle, elle doit transférer les données exactes vers une étiquette RFID. L'étiquette est ensuite attachée à un objet tel qu'une carte, un porte-clés ou un badge.
- **Présentation de la carte RFID.** Le visiteur attendu doit disposer d'une carte RFID (ou tout autre objet de son choix contenant ses tags RFID uniques).

Vous devez noter que la plupart des systèmes de contrôle RFID sont hautement automatisés. Il est peu probable que vous ayez un assistant à la porte. Cependant, le lecteur RFID détectera immédiatement votre étiquette RFID et ouvrira la porte pour vous permettre d'accéder aux locaux sans restrictions.

Autorisation des données

C'est la dernière étape des systèmes de contrôle RFID. Cela implique l'analyse et l'authentification des données. Le système dispose d'un panneau de contrôle avec une mémoire contenant les détails de tous les visiteurs/employés attendus.

Lorsqu'un individu s'approche de la porte, la séquence d'événements suivante se produit :

- **L'étiquette RFID est alimentée.** Le lecteur RFID, généralement placé à la porte, libère des signaux électromagnétiques. Lorsque l'étiquette reçoit ces signaux, elle est alimentée et envoie les informations enregistrées au lecteur.
- **Le lecteur RFID reçoit des données.** Le lecteur est livré avec une antenne qui reçoit et transmet des données. Dès qu'il reçoit les données, ce lecteur les envoie au panneau de contrôle pour analyse.
- **Comparaison des données.** Lorsque la centrale reçoit des données du lecteur, elle parcourt sa base de données. Si les données envoyées correspondent à d'autres données disponibles sur la liste blanche, la porte s'ouvrira automatiquement.

Si l'une de ces actions est interrompue, le système ne fonctionnera pas. Si vous rencontrez des difficultés d'accès malgré une carte RFID valide, vous devrez vous renseigner auprès de la direction. Les deux scénarios possibles seraient des données erronées copiées sur la carte ou un dysfonctionnement du système.

Avantages et inconvénients du système de contrôle d'accès RFID

Les systèmes de contrôle d'accès RFID présentent de nombreux avantages en matière de sécurité pour une organisation. Ils garantissent que seules les personnes autorisées peuvent accéder aux locaux donnés.

Il aide également une organisation à attribuer des rôles spécifiques à des employés spécifiques. En tant que tel, il est plus facile de prévenir les violations de données car les employés seront responsables de chaque action qu'ils entreprendront en service.

De plus, les cartes RFID sont durables. Il peut résister à des environnements difficiles, ce qui les rend plus rentables que d'autres alternatives telles que les codes-barres.

Cependant, les systèmes d'accès RFID présentent également plusieurs inconvénients. Par exemple, il y a des chances que le système soit piraté, ce qui peut entraîner la fuite de données privées. Ils peuvent également être clonés au cas où des pirates obtiendraient des détails sur la carte. Heureusement, le Les étiquettes RFID peut facilement être désactivé, évitant ainsi la peur de l'utilisation par les cybercriminels.

Extrait du décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature

Le Premier ministre,
Sur le rapport de la ministre de la décentralisation et de la fonction publique,(...)

Le Conseil d'Etat (section de l'administration) entendu,
Décrète :

[Article 1](#)

Les dispositions du présent décret s'appliquent aux fonctionnaires et aux agents publics non fonctionnaires régis par la [loi du 13 juillet 1983 susvisée](#) et aux magistrats de l'ordre judiciaire régis par l'[ordonnance du 22 décembre 1958 susvisée](#).

[Article 2](#)

Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux où il est affecté sont réalisées hors de ces locaux en utilisant les technologies de l'information et de la communication.

Le télétravail peut être organisé au domicile de l'agent, dans un autre lieu privé ou dans tout lieu à usage professionnel.

Un agent peut bénéficier au titre d'une même autorisation de ces différentes possibilités.

Les périodes d'astreintes mentionnées à l'[article 5 du décret du 25 août 2000 susvisé](#), à l'[article 5 du décret du 12 juillet 2001 susvisé](#) et à l'[article 20 du décret du 4 janvier 2002 susvisé](#) ne constituent pas du télétravail au sens du présent décret.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

[Article 2-1](#)

L'autorisation de télétravail est délivrée pour un recours régulier ou ponctuel au télétravail. Elle peut prévoir l'attribution de jours de télétravail fixes au cours de la semaine ou du mois ainsi que l'attribution d'un volume de jours flottants de télétravail par semaine, par mois ou par an dont l'agent peut demander l'utilisation à l'autorité responsable de la gestion de ses congés.

Un agent peut, au titre d'une même autorisation, mettre en œuvre ces différentes modalités de télétravail.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

[Article 3](#)

La quotité des fonctions pouvant être exercées sous la forme du télétravail ne peut être supérieure à trois jours par semaine. Le temps de présence sur le lieu d'affectation ne peut être inférieur à deux jours par semaine.

Les seuils définis au premier alinéa peuvent s'apprécier sur une base mensuelle.

[Article 4](#)

Il peut être dérogé aux conditions fixées à l'article 3 :

1° Pour une durée de six mois maximum, à la demande des agents dont l'état de santé ou le handicap le justifient et après avis du service de médecine préventive ou du médecin du travail ; cette dérogation est renouvelable, après avis du service de médecine préventive ou du médecin du travail ;

2° A la demande des femmes enceintes ;

3° A la demande des agents éligibles au congé de proche aidant prévu à l'article L. 3142-16 du code du travail, pour une durée de trois mois maximum, renouvelable ;

4° Lorsqu'une autorisation temporaire de télétravail a été demandée et accordée en raison d'une situation exceptionnelle perturbant l'accès au service ou le travail sur site.

Se reporter aux conditions d'application prévues à l'article 2 du décret n° 2021-1725 du 21 décembre 2021.

[Article 5](#)

L'exercice des fonctions en télétravail est accordé sur demande écrite de l'agent. Celle-ci précise les modalités d'organisation souhaitées. Lorsque le télétravail est organisé au domicile de l'agent ou dans un autre lieu privé, une attestation de conformité des installations aux spécifications techniques, établie conformément aux dispositions prises en application du 9° du I de l'article 7, est jointe à la demande.

Le chef de service, l'autorité territoriale ou l'autorité investie du pouvoir de nomination apprécie la compatibilité de la demande avec la nature des activités exercées et l'intérêt du service. Lorsque l'autorité investie du pouvoir de nomination est le Centre national de gestion, cette appréciation est assurée :

1° Par le chef d'établissement pour les directeurs adjoints et les directeurs des soins ;

2° Par le directeur général de l'agence régionale de santé pour les chefs des établissements mentionnés aux 1°, 3° et 5° de l'article 2 de la loi du 9 janvier 1986 susvisée ;

3° Par le préfet du département pour les établissements mentionnés aux 4° et 6° du même article 2.

Une réponse écrite est donnée à la demande de télétravail dans un délai d'un mois maximum à compter de la date de sa réception ou de la date limite de dépôt lorsqu'une campagne de recensement des demandes est organisée.

En cas de changement de fonctions, l'agent intéressé doit présenter une nouvelle demande.

L'autorisation peut prévoir une période d'adaptation de trois mois maximum.

Il peut être mis fin à cette forme d'organisation du travail, à tout moment et par écrit, à l'initiative de l'administration ou de l'agent, moyennant un délai de prévenance de deux mois. Dans le cas où il est mis fin à l'autorisation de télétravail à l'initiative de l'administration, le délai de prévenance peut être réduit en cas de nécessité du service dûment motivée. Pendant la période d'adaptation, ce délai est ramené à un mois.

Le refus opposé à une demande d'autorisation de télétravail ainsi que l'interruption du télétravail à l'initiative de l'administration doivent être motivés et précédés d'un entretien.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

[Article 6](#)

Les agents exerçant leurs fonctions en télétravail bénéficient des mêmes droits et obligations que les agents exerçant sur leur lieu d'affectation.

L'employeur prend en charge les coûts découlant directement de l'exercice des fonctions en télétravail, notamment le coût des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci. L'employeur n'est pas tenu de prendre en charge le coût de la location d'un espace destiné au télétravail.

Dans le cas où la demande est formulée par un agent en situation de handicap, le chef de service, l'autorité territoriale ou l'autorité investie du pouvoir de nomination ou, à défaut, selon les cas, l'une des autorités mentionnées aux troisième, quatrième et cinquième alinéas de l'article 5, met en œuvre sur le lieu de télétravail de l'agent les aménagements de poste nécessaires, sous réserve que les charges consécutives à la mise en œuvre de ces mesures ne soient pas disproportionnées, notamment compte tenu des aides qui peuvent compenser, en tout ou partie, les dépenses engagées à ce titre par l'employeur.

Lorsqu'un agent demande l'utilisation des jours flottants de télétravail ou l'autorisation temporaire de télétravail mentionnée au 2° de l'article 4, l'administration peut autoriser l'utilisation de l'équipement informatique personnel de l'agent.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 7

Un arrêté ministériel pour la fonction publique de l'Etat, une délibération de l'organe délibérant pour la fonction publique territoriale, une décision de l'autorité investie du pouvoir de nomination pour la fonction publique hospitalière, pris après avis du comité technique ou du comité consultatif national compétent, fixe :

- 1° Les activités éligibles au télétravail ;
- 2° La liste et la localisation des locaux professionnels éventuellement mis à disposition par l'administration pour l'exercice des fonctions en télétravail, le nombre de postes de travail qui y sont disponibles et leurs équipements ;
- 3° Les règles à respecter en matière de sécurité des systèmes d'information et de protection des données ;
- 4° Les règles à respecter en matière de temps de travail, de sécurité et de protection de la santé ;
- 5° Les modalités d'accès des institutions compétentes sur le lieu d'exercice du télétravail afin de s'assurer de la bonne application des règles applicables en matière d'hygiène et de sécurité ;
- 6° Les modalités de contrôle et de comptabilisation du temps de travail ;
- 7° Les modalités de prise en charge, par l'employeur, des coûts découlant directement de l'exercice du télétravail, notamment ceux des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci ;
- 8° Les modalités de formation aux équipements et outils nécessaires à l'exercice du télétravail ;
- 9° Les conditions dans lesquelles l'attestation mentionnée à l'article 5 est établie.

Lorsque l'autorité investie du pouvoir de nomination est le Centre national de gestion, la décision fixant

Les modalités et règles mentionnées au présent I est prise :

- 1° Par le chef d'établissement pour les directeurs adjoints et les directeurs des soins ;
- 2° Par le directeur général de l'agence régionale de santé pour les chefs des établissements mentionnés aux 1°, 3° et 5° de l'article 2 de la loi du 9 janvier 1986 susvisée ;
- 3° Par le préfet du département pour les établissements mentionnés aux 4° et 6° du même article 2.

La décision n'est pas soumise à l'avis du comité consultatif national.

II. - Dans les directions départementales interministérielles, les conditions de mise en œuvre du télétravail prévues au I font l'objet d'un arrêté du Premier ministre, pris après avis du comité technique des directions départementales interministérielles.

III. - Les modalités de mise en œuvre du télétravail fixées aux 1° à 9° du I sont précisées en tant que de besoin, dans chaque service ou établissement, après consultation du comité technique ou du comité consultatif national compétent.

IV. - Les comités d'hygiène, de sécurité et des conditions de travail compétents et la commission des conditions de travail commune aux personnels de direction de la fonction publique hospitalière sont informés des avis rendus par les comités techniques ou le comité consultatif national en application du présent article.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 8

I. - L'autorisation d'exercice des fonctions en télétravail mentionne :

- 1° Les fonctions de l'agent exercées en télétravail ;
- 2° Le lieu ou les lieux d'exercice en télétravail ;
- 3° Les modalités de mise en œuvre du télétravail et, s'il y a lieu, sa durée, ainsi que les plages horaires durant lesquelles l'agent exerçant ses activités en télétravail est à la disposition de son employeur et peut être joint, par référence au cycle de travail de l'agent ou aux amplitudes horaires de travail habituelles ;
- 4° La date de prise d'effet de l'exercice des fonctions en télétravail ;

5° Le cas échéant, la période d'adaptation prévue à l'article 5 et sa durée.

II. - Lors de la notification de l'autorisation d'exercice, l'autorité mentionnée à l'article 5 remet à l'agent intéressé :

1° Un document d'information indiquant les conditions d'application à sa situation professionnelle de l'exercice des fonctions en télétravail, notamment :

- a) La nature et le fonctionnement des dispositifs de contrôle et de comptabilisation du temps de travail ;
- b) La nature des équipements mis à disposition de l'agent exerçant ses activités en télétravail et leurs conditions d'installation et de restitution, les conditions d'utilisation, de renouvellement et de maintenance de ces équipements et de fourniture, par l'employeur, d'un service d'appui technique ;

2° Une copie des règles mentionnées à l'article 7 et un document rappelant ses droits et obligations en matière de temps de travail et d'hygiène et de sécurité.

Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.