Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 32121**

Intitulé

Architecte réseaux et cybersécurité (MS)

AUTORITÉ RESPONSABLE DE LA CERTIFICATION	QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION
Institut Mines Télécom - Télécom ParisTech	Directeur

Niveau et/ou domaine d'activité

I (Nomenclature de 1969)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

326 Informatique, traitement de l'information, réseaux de transmission

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

L'architecte réseaux et cybersécurité est un métier essentiel dans les organisations modernes. Son expertise lui permet de piloter la conception d'une architecture réseau (la partie matérielle du réseau), de définir l'architecture d'un système d'information (la partie logicielle) et de créer une architecture de cybersécurité, prenant en compte les choix fait au niveau du réseau et du système d'information.

Activités visées par le titre :

Réalisation de l'architecture d'un réseau télécom de transport de données

Réalisation de l'architecture d'un système d'information ou d'un service applicatif

Réalisation de l'architecture cybersécurisée d'un réseau ou d'un système d'information

Pilotage et réalisation d'un projet du domaine de la cybersécurité

Réaliser l'architecture d'un réseau télécom de transport de données sur la base des besoins du client interne ou externe et des enjeux de sécurité et d'évolution future

Réaliser l'architecture d'un système d'information ou d'un service applicatif de manière à assurer son fonctionnement pérenne et ses évolutions selon les besoins du client

Réaliser l'architecture cybersécurisée d'un réseau ou d'un SI en mettant en œuvre des méthodes et techniques préventives et palliatives, répondant aux enjeux de sécurité et aux obligations légales du client

Piloter et réaliser un projet de développement de la cybersécurité d'un réseau ou d'un SI, en s'appuyant sur des équipes techniques internes et des sous-traitants

Secteurs d'activité ou types d'emplois accessibles par le détenteur de ce diplôme, ce titre ou ce certificat

L'architecte réseaux et cybersécurité est amené à travailler dans les grandes entreprises, les opérateurs télécoms, les constructeurs ou équipementiers télécoms, les sociétés de services numériques (ESN). De façon générale, il peut exercer ses activités dans les DSI (direction du service d'information) de n'importe quelle entreprise de taille suffisante.

Architecte réseaux, Architecte cybersécurité et blockchain, Responsable sécurité informatique, Chef de projet SI, Analystes et experts réseaux et SI

Codes des fiches ROME les plus proches :

M1801 : Administration de systèmes d'information

M1802 : Expertise et support en systèmes d'information

M1803 : Direction des systèmes d'information

M1804 : Études et développement de réseaux de télécoms

M1806 : Conseil et maîtrise d'ouvrage en systèmes d'information

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

La certification comporte 4 composantes :

Réaliser l'architecture d'un réseau télécom de transport de données

Réaliser l'architecture d'un système d'information ou d'un service applicatif

Réaliser l'architecture cybersécurisée d'un réseau ou d'un système d'information

Piloter et réaliser un projet du domaine de la cybersécurité

La certification est composée de 4 blocs de compétences décrits ci-dessuos. Si un candidat souhaite obtenir la certification, il doit valider obligatoirement les blocs d'activité, remplir les conditions d'accès fixées par la CGE, et faire approuver sa thèse professionnelle.

Bloc de compétence :

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°1 de la fiche n° 32121 - Réaliser l'architecture d'un système d'information ou d'un service applicatif de manière à assurer son fonctionnement pérenne et ses évolutions à venir, selon les besoins du client	**Compétences évaluées :** *• Décrire le modèle de représentation du SI le plus conforme aux besoins, en soumettant des solutions pour adapter le réseau de l'entreprise en conséquence* *• Définir une organisation pour assurer le maintien en bon fonctionnement du SI et son évolution, en respectant la structure existante et les contraintes qui lui sont liées* *• Définir les performances applicatives relatives à l'évolution du SI, de façon à adapter l'écosystème du Cloud selon le contrat de service, et faire valoir les arguments auprès de la direction* **Modalités d'évaluation :** • Tests d'acquisition des connaissances, ou QCM (questions à choix multiples) • Projets pédagogiques : projet d'une conception technique et sécurisée d'un service, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement • Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : mise en place d'une solution SI sécurisée

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°2 de la fiche n° 32121 - Réaliser l'architecture cybersécurisée d'un réseau ou d'un SI en mettant en œuvre des méthodes et techniques préventives et palliatives, répondant aux enjeux de sécurité et aux obligations légales	**Compétences évaluées :** *• Mettre en œuvre une méthode adaptée, en fonction du SI, de restitution des failles de sécurité, en signalant des recommandations plausibles, selon le contexte de l'entreprise* *• Mettre en œuvre des solutions techniques et organisationnelles pour pallier les risques élémentaires, en élaborant les solutions de contrôle des accès, et en protégeant le réseau de la corruption des données* *• Mettre en place une architecture cybersécurisée qui puisse détecter et filtrer les programmes malveillants, afin de lutter contre les menaces persistantes avancées* **Modalités d'évaluation** • Tests d'acquisition des connaissances, ou QCM (questions à choix multiples) • Projets pédagogiques : projet d'une conception technique et sécurisée d'un service, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement • Cas pratique : conception d'une architecture de sécurité, mise en place d'un audit de sécurité • Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : mise en place d'une solution SI sécurisée

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°3 de la fiche n° 32121 - Piloter un projet de développement de la cybersécurité d'un réseau et / ou d'un SI, en s'appuyant sur des équipes techniques internes et des sous-traitants	**Compétences évaluées :** *• Elaborer un plan de recrutement de l'équipe projet, en s'appuyant sur les enjeux, les produits à livrer, les contraintes de coût, délai et qualité identifiés, afin d'obtenir l'accord de la hiérarchie* *• Etablir les critères de sélection des fournisseurs en prenant en compte les objectifs de réalisation du projet, les besoins exprimés, et en analysant les transcrits des soutenances* *• Réaliser le plan de gestion du projet, en ordonnançant les tâches, en dressant une cartographie réaliste des risques et des palliatifs, en déterminant les éléments de coût-délai-qualité, et en communiquant sur les actions mises en œuvre* **Modalités d'évaluation :** • Tests d'acquisition des connaissances, ou QCM (questions à choix multiples) • Projet pédagogique : réponse à l'appel d'offres d'un client • Cas pratique : conception d'une architecture de sécurité • Travaux de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : élaboration d'une architecture télécom, fixe ou mobile, mise en place d'une solution SI sécurisée, définition du calendrier des processus du projet, organisationnels et techniques, description des livrables d'un projet

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°4 de la fiche n° 32121 - Réaliser l'architecture d'un réseau télécom de transport de données, sur la base des besoins du client interne ou externe, des enjeux de sécurité et des évolutions à venir	***Compétences évaluées :*** *• Analyser et élaborer une architecture de réseau d'entreprise, de réseau d'accès fixe, et de réseau cœur de transport, cuivre, optique ou hertzien, en considérant les évolutions de trafic, du matériel, et de la technologie.* *• Analyser et élaborer une architecture de réseau radiomobile de type 4G, en prenant en compte le développement de la capacité des trafics, et en anticipant les évolutions vers la 5G, notamment celles liées aux services des objets connecté.* *• Définir les solutions vraisemblables aux dysfonctionnements courants de la qualité de service, notamment ceux liés aux flux du trafic et à la garantie de l'accès au service.* **Modalités d'évaluation :** • Tests d'acquisition des connaissances, ou QCM (questions à choix multiples) • Projets pédagogiques : réponse à l'appel d'offres d'un client, projet relatif aux dispositions à respecter pour le maintien d'un service en bon fonctionnement. • Cas pratique : atelier de sécurisation d'un réseau mobile • Travail de réflexion et d'analyse sur la base d'un cas réel en entreprise, en immersion professionnelle : élaboration d'une architecture télécom, fixe ou mobile.

Validité des composantes acquises : non prévue

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUI	NON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant	X		6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés
En contrat d'apprentissage		X	
Après un parcours de formation continue	X		6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés
En contrat de professionnalisation	X		6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés
Par candidature individuelle		X	
Par expérience dispositif VAE prévu en 2013	X		Par VAE, 6 personnes au total, dont 2 professionnels et 2 anciens titulaires de la certification, salariés

	OUI	NON
Accessible en Nouvelle Calédonie		X
Accessible en Polynésie Française		X

LIENS AVEC D'AUTRES CERTIFICATIONS	ACCORDS EUROPÉENS OU INTERNATIONAUX

Base légale

Référence du décret général :

Référence arrêté création (ou date 1er arrêté enregistrement) :

Arrêté du 27 décembre 2018 publié au Journal Officiel du 4 janvier 2019 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour cinq ans, au niveau I, sous l'intitulé « Architecte réseaux et cybersécurité (MS) » avec effet au 1er décembre 2014 , jusqu'au 4 janvier 2024.

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

12 certifiés en moyenne par an sur les 3 dernières années, effectifs croissants d'année en année

Autres sources d'information :

« Les formations et les compétences en France sur la cybersécurité », étude FAFIEC, mai 2017 - www.fafiec.fr

Site de Télécom ParisTech pour le MS

Lieu(x) de certification :

Institut Mines Télécom - Télécom ParisTech : Île-de-France - Paris (75) [Dareau]

Télécom ParisTech – 75014 Paris (37/39 rue Dareau)

Lieu(x) de préparation à la certification déclarés par l'organisme certificateur :

Télécom ParisTech – 75014 Paris (37/39 rue Dareau)

Historique de la certification :

Accréditation CGE initiale en 1998, avec le titre « Réseaux : option sécurité »

Premier changement de titre « Architecte réseaux et sécurité (ARS) », autorisé le 16 janvier 2012

Nouveau changement de titre « Architecte réseaux et cybersécurité (ARC) » autorisé pour 6 ans, à compter du 1er septembre 2017 (décision 2988/0517/CGE/FJ/GC)