

Concepteur de systèmes IoT sécurisés (MS)

RNCP40345 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	110, 255n, 326
Formacode(s)	24323, 24307, 24308, 31032
Code(s) ROME	H1206
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	28/03/2025
Date d'échéance	28/03/2028

Certificateur(s)

INSTITUT MINES TELECOM - ECOLE NATIONALE SUPERIEURE DES MINES SAINT ETIENNE · SIRET : 18009202500105

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former.

Organisme	SIRET	Habilitation
FORMA SUP ARL	43903961100025	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification vise à apporter une double compétences à des apprenants déjà experts en particulier, en électronique, informatique, micro-électronique, mécanique...afin qu'ils intègrent dès la conception d'un d'objet connecté les spécifications de cyber sécurité liés à l'usage de cet objet, pour le rendre le moins attaquable possible et le plus respectueux de la protection et la confidentialité des données pour déjouer toute action malveillante et préjudiciable. La maîtrise de la juste consommation d'énergie embarquée sur la carte électronique est aussi un enjeu de sobriété énergétique.

ACTIVITÉS VISÉES

Réaliser le prototype physique de l'objet connecté

- Rédaction des spécifications d'un objet connecté
- Conception de l'objet connecté
- Réalisation du prototypage de l'objet connecté
- Réalisation des tests de la faisabilité des fonctionnalités de l'objet connecté

Réaliser le prototype de la sécurisation de l'objet connecté

- Sécurisation par la cryptographie
- Détermination des niveaux de cybersécurité et des normes de certification
- Exploitation Vérification de l'audit de sécurité et des préconisations associées

Réaliser la connectivité sécurisée de l'objet connecté

- Conception de l'application et l'infrastructure nécessaire réseau nécessaire pour l'utilisation et la communication des données produites par l'objet connecté
- Déploiement des protocoles réseaux

Réaliser les tests pour un objet sécurisé et robuste prêt pour la phase de pré-industrialisation

- Gestion de la veille technologique
- Gestion des tests de sécurité au regard des normes
- Validation de la fiabilité et de la robustesse de l'objet connecté

Manager des projets de conception d'un système IoT sécurisé

- Management de projet
- Présentation argumentée des choix technologiques aux décideurs

COMPÉTENCES ATTESTÉES

Identifier les usages en conditions normales de l'objet connecté en sollicitant les utilisateurs finaux qui incluent, les personnes en situation de handicap, afin de déterminer les fonctionnalités et les spécifications techniques de l'objet connecté à fabriquer

Concevoir les fonctionnalités de l'objet connecté adaptées aussi aux besoins des personnes en situation de handicap en s'appuyant sur les spécifications techniques afin de préfigurer le prototype de l'objet connecté

Identifier les capteurs les plus performants pour construire le flux et la gestion des données en s'appuyant sur la connaissance des experts pour sélectionner les capteurs idoines

Définir un profil d'usage sécuritaire en prenant en compte les usages et l'évaluation de sécurité attendue face aux attaques physiques, afin de préfigurer le juste niveau de sécurité au juste coût.C.5.Schématiser et concevoir l'ensemble des architectures électronique, numérique et de la donnée avec les experts techniques et technologiques en s'appuyant sur les spécifications techniques afin de préfigurer le prototype de l'objet connecté

Identifier les capteurs les plus performants en fonction des usages de l'IoT pour construire le flux et la gestion des données en s'appuyant sur la connaissance des experts pour sélectionner les capteurs les plus efficaces

Définir un algorithme de sécurisation sur le microcontrôleur en optimisant sa programmation afin qu'il soit le moins énergivore possible

Tester et re-designer le prototype en itérant les versions afin d'aboutir à la preuve de concept validée de l'objet connecté

Réaliser l'architecture matérielle, logicielle électronique et numérique avec les experts techniques et technologiques en se référant à la validation de la simulation afin de fabriquer le prototype de l'objet connecté

Réaliser l'architecture de la donnée depuis le capteur physique jusqu'à son traitement en se référant à la validation de la simulation afin de fabriquer le prototype de l'objet connecté

Réaliser le prototype physique de l'objet connecté qui intègre l'ensemble des architectures, les capteurs ainsi que le design de l'objet connecté en s'appuyant sur l'équipe de conception de l'objet connecté afin de présenter à l'utilisateur final une version fonctionnelle pré-industrielle

Tester la fonctionnalité des architectures matérielle, logicielle, électronique, numérique, de la donnée et des capteurs embarqués en déployant une série de tests qualifiés afin de démontrer la fiabilité et le bon fonctionnement de l'objet connecté selon les usages attendus

Réaliser les tests de validité du dispositif assemblé afin d'aboutir à la version certifiée pour passer en phase de pré-industrialisation

Déployer le protocole de cryptographie en prévoyant la gestion des clefs de chiffrement/déchiffrement afin de sécuriser l'objet connecté

Identifier les mécanismes, les outils d'intrusion et de cyberattaques tant sur les réseaux informatiques que l'objet en tant que tel en répertoriant les typologies d'attaques possibles afin de sécuriser tout le dispositif

Établir une veille technologique en suivant les évolutions en matière de cyberattaques afin d'intégrer les mises à jour au dispositif le plus sécurisé face aux menaces cyber.C.16. Concevoir la meilleure stratégie d'anticipation de réponse adaptée aux différents types de cyberattaques et d'intrusion en sachant sélectionner les protocoles et les standards internationalement reconnus afin de réduire les risques d'attaques et d'intrusion des systèmes d'information et de l'objet connecté pour en maintenir le bon fonctionnement

Défendre le choix de la solution technique de cybersécurité utilisée en démontrant son bénéfice risque aux organes décisionnaires, afin de leur apporter les éléments de prise de décisions objectifs

Déployer la stratégie cybersécurité en réalisant des audits de système d'information et de réseaux d'objets connectés afin de valider la fiabilité de l'infrastructure et des solutions déployées sur le système d'information comme l'objet connecté et apporter le cas échéant les mesures correctives conformes aux standards et normes en vigueur.

Définir la cible de sécurité au regard de l'usage de l'objet connecté en maîtrisant le coût de la certification afin de la déployer

Intégrer l'analyse des comptes rendus des critères communs et certifications de premier niveau de l'ANSSI en considérant les attentes du fournisseur afin de réaliser le prototype de sécurisation de l'objet connecté

Analyser l'audit des normes de sécurité et de sûreté de fonctionnement en conduisant des essais ou en lisant les rapports de certification, afin de vérifier le respect par l'objet connecté audité de ces normes

Valider le niveau de sécurité de l'objet connecté, en préconisant éventuellement des mesures correctives afin de les mettre en place

Implémenter la représentation des données choisies ou des spécifications des protocoles en les auditant après analyse, afin d'opérer ainsi un choix entre concevoir les programmes ou utiliser des bibliothèques existantes

Caractériser les fonctionnalités des différents composants en les sélectionnant en amont, afin de déterminer les couches de communication et la sécurisation déjà incluses ou qui sont à rajouter en fonction des usages de l'objet connecté

Implémenter les spécifications définies lors de la phase de conception en apportant les mesures correctives nécessaires afin d'aboutir à un prototype validé

Concevoir la maquette de l'environnement réaliste des échanges de données en instrumentant tous les échanges et en déterminant les caractéristiques de l'objet en fonction des contraintes de communication afin déployer cette maquette

Déployer une infrastructure de type linux ou tcpip ou bare metal à partir des ressources allouées (Financière, énergétique, matérielle) en adaptant le hardware aux besoins afin de définir les priorités.

Déployer des outils de spécifications et vérifications formelles de sécurité en construisant la méthode pour exprimer le lien entre sécurité et sûreté, afin de prouver cette méthode formelle

Construire l'architecture de la plateforme de l'objet connecté en structurant les différentes couches de collecte et de données générées par les capteurs afin de configurer la communication d'un réseau de capteurs.

Concevoir l'infrastructure logicielle en utilisant les bases de données relationnelles NoSQL, les technologies edge et cloud afin de l'interfacer avec le réseau d'objets connecté

Assurer la veille technologique et réglementaire, en s'assurant que les protocoles et les standards déployés sont bien dans leur dernière mise à jour afin de maintenir une plateforme et un système continuellement à jour pour contrer tous types d'attaques

Définir précisément, le périmètre de la cible de sécurité de l'objet connecté en définissant son contenu et sa structure afin que l'organe de sécurité puisse valider en conséquence

Déterminer les tests d'intrusion adéquats en s'appuyant sur la typologie d'objet connecté et de ses usages afin de déployer la série de tests définie

Déterminer la récurrence de ces tests en prenant en compte les conditions d'usage de l'objet connecté afin de réduire le risque d'attaques

Sensibiliser les utilisateurs en les formant à la politique de cybersécurité afin de développer une culture de la sécurité au sein des organisations

Choisir les tests idoines en prenant en compte les normes vieillissement, de compatibilité électromagnétique, des normes liées aux usages définis par le cahier des charges fonctionnelles afin de réaliser les tests

Valider la robustesse et la fiabilité de l'objet connecté en assurant sa recette et délivrer la certification sécurité afin de passer à la phase d'industrialisation

Animer l'équipe pluridisciplinaire et multiculturelle en identifiant toutes les expertises techniques et technologiques requises afin de concevoir l'objet connecté sécurisé conforme aux usages attendus

Déployer les outils de conduite de projet en maîtrisant les coûts, la qualité et les délais, de la conception de l'objet connecté afin de répondre au contrat passé avec le client

Manager de manière inclusive les collaborateurs en situation de handicap par exemple, en adaptant les missions des collaborateurs afin qu'ils atteignent les résultats attendus

Etre à l'écoute des problématiques liées aux handicaps en démontrant une action proactive en la matière afin de faciliter l'intégration des collaborateurs

.Déployer une stratégie de cybersécurité en formant toutes les parties prenantes internes et externes de l'organisation aux enjeux afin qu'elle soit acceptée et mise en œuvre

Défendre le choix technique et économique de la solution de cybersécurité choisie en en justifiant sa démarche et en démontrant son bénéfice risque afin que les décideurs arrêtent une stratégie financière et commerciale viable pour le déploiement de l'objet connecté

Blocs de compétences

RNCP40345BC01 — Réaliser le prototype physique de l'objet connecté

LISTE DE COMPÉTENCES

Identifier les usages en conditions normales de l'objet connecté en sollicitant les utilisateurs finaux qui incluent, les personnes en situation de handicap, afin de déterminer les fonctionnalités et les spécifications techniques de l'objet connecté à fabriquer

Concevoir les fonctionnalités de l'objet connecté adaptées aussi aux besoins des personnes en situation de handicap en s'appuyant sur les spécifications techniques afin de préfigurer le prototype de l'objet connecté

Identifier les capteurs les plus performants pour construire le flux et la gestion des données en s'appuyant sur la connaissance des experts pour sélectionner les capteurs idoines

Définir un profil d'usage sécuritaire en prenant en compte les usages et l'évaluation de sécurité attendue face aux attaques physiques, afin de préfigurer le juste niveau de sécurité au juste coût

Schématiser et concevoir l'ensemble des architectures électronique, numérique et de la donnée avec les experts techniques et technologiques en s'appuyant sur les spécifications techniques afin de préfigurer le prototype de l'objet connecté

Identifier les capteurs les plus performants en fonction des usages de l'IoT pour construire le flux et la gestion des données en s'appuyant sur la connaissance des experts pour sélectionner les capteurs les plus efficaces

Définir un algorithme de sécurisation sur le microcontrôleur en optimisant sa programmation afin qu'il soit le moins énergivore possible

Tester et re-designer le prototype en itérant les versions afin d'aboutir à la preuve de concept validée de l'objet connecté.

Réaliser l'architecture matérielle, logicielle électronique et numérique avec les experts techniques et technologiques en se référant à la validation de la simulation afin de fabriquer le prototype de l'objet connecté

Réaliser l'architecture de la donnée depuis le capteur physique jusqu'à son traitement en se référant à la validation de la simulation afin de fabriquer le prototype de l'objet connecté

Réaliser le prototype physique de l'objet connecté qui intègre l'ensemble des architectures, les capteurs ainsi que le design de l'objet connecté en s'appuyant sur l'équipe de conception de l'objet connecté afin de présenter à l'utilisateur final une version fonctionnelle pré-industrielle

Tester la fonctionnalité des architectures matérielle, logicielle, électronique, numérique, de la donnée et des capteurs embarqués en déployant une série de tests qualifiés afin de démontrer la fiabilité et le bon fonctionnement de l'objet connecté selon les usages attendus

Réaliser les tests de validité du dispositif assemblé afin d'aboutir à la version certifiée pour passer en phase de pré-industrialisation

MODALITÉS D'ÉVALUATION

Evaluation 1 :

Travaux Pratiques en équipe qui permettent d'appliquer les compétences C1 à C13.

Ces travaux pratiques se réalisent sur des équipements techniques industriels

Production d'un prototype physique étape par étape et présentation à l'oral : Travail collectif

Evaluation 2 :

Mini-projet de prototypage d'un système IoT de l'objet connecté au cloud avec sa base de données, son IHM qui permet d'appliquer compétences C5 à C13.

Production d'un prototype physique complet et en fonctionnement nominal et présentation à l'oral : Travail collectif

Evaluation 3 :

Mission en entreprise intégrant une activité de définition de cahier des charges, de conception ou de réalisation d'un prototype physique d'un objet connecté

Production d'un mémoire suivi d'une présentation orale

RNCP40345BC02 — Réaliser le prototype de la sécurisation logicielle de l'objet connecté

LISTE DE COMPÉTENCES

Déployer le protocole de cryptographie en prévoyant la gestion des clefs de chiffrement/déchiffrement afin de sécuriser l'objet connecté

Identifier les mécanismes, les outils d'intrusion et de cyberattaques tant sur les réseaux informatiques que l'objet en tant que tel en répertoriant les typologies d'attaques possibles afin de sécuriser tout le dispositif

Établir une veille technologique en suivant les évolutions en matière de cyberattaques afin d'intégrer les mises à jour au dispositif le plus sécurisé face aux menaces cyber.

internationalement reconnus afin de réduire les risques d'attaques et d'intrusion des systèmes d'information et de l'objet connecté pour en maintenir le bon fonctionnement

Défendre le choix de la solution technique de cybersécurité utilisée en démontrant son bénéfice risque aux organes décisionnaires, afin de leur apporter les éléments de prise de décisions objectivés

Déployer la stratégie cybersécurité en réalisant des audits de système d'information et de réseaux d'objets connectés afin de valider la fiabilité de l'infrastructure et des solutions déployées sur le système d'information comme l'objet connecté et apporter le cas échéant les mesures correctives conformes aux standards et normes en vigueur.

Définir la cible de sécurité au regard de l'usage de l'objet connecté en maîtrisant le coût de la certification afin de la déployer

Intégrer l'analyse des comptes rendus des critères communs et certifications de premier niveau de l'ANSSI en considérant les attentes du fournisseur afin de réaliser le prototype de sécurisation de l'objet connecté

Analyser l'audit des normes de sécurité et de sûreté de fonctionnement en conduisant des essais ou en lisant les rapports de certification, afin de vérifier le respect par l'objet connecté audité de ces normes

Valider le niveau de sécurité de l'objet connecté, en préconisant éventuellement des mesures correctives afin de les mettre en place

MODALITÉS D'ÉVALUATION

Evaluation 1 :

Travaux pratiques avec mise en œuvre expérimentale, réalisés en groupe ou individuellement. Ils permettent d'appliquer les compétences de C14 à C23.

Ces travaux pratiques se réalisent sur des équipements techniques industriels.

Production du prototype de sécurisation de l'objet connecté avec remise d'un rapport écrit.

Evaluation 2 :

Mission en entreprise intégrant une activité de définition de cahier des charges, de conception ou de réalisation d'un prototype de la sécurisation d'un objet connecté

Production d'un mémoire suivi d'une présentation orale

RNCP40345BC03 — Réaliser la connectivité sécurisée de l'objet connecté

LISTE DE COMPÉTENCES

Implémenter la représentation des données choisies ou des spécifications des protocoles en les auditant après analyse, afin d'opérer ainsi un choix entre concevoir les programmes ou utiliser des bibliothèques existantes

Caractériser les fonctionnalités des différents composants en les sélectionnant en amont, afin de déterminer les couches de communication et la sécurisation déjà incluses ou qui sont à rajouter en fonction des usages de l'objet connecté

Implémenter les spécifications définies lors de la phase de conception en apportant les mesures correctives nécessaires afin d'aboutir à un prototype validé

Concevoir la maquette de l'environnement réaliste des échanges de données en instrumentant tous les échanges et en déterminant les caractéristiques de l'objet en fonction des contraintes de communication afin déployer cette maquette

.Déployer une infrastructure de type linux ou tcpip ou bare metal à partir des ressources allouées (Financière, énergétique, matérielle) en adaptant le hardware aux besoins afin de définir les priorités.

Déployer des outils de spécifications et vérifications formelles de sécurité en construisant la méthode pour exprimer le lien entre sécurité et sûreté, afin de prouver cette méthode formelle

Construire l'architecture de la plateforme de l'objet connecté en structurant les différentes couches de collecte et de données générées par les capteurs afin de configurer la communication d'un réseau de capteurs.

Concevoir l'infrastructure logicielle en utilisant les bases de données relationnelles NoSQL, les technologies edge et cloud afin de l'interfacer avec le réseau d'objets connecté

MODALITÉS D'ÉVALUATION

Evaluation 1 :

Mini-projet en groupe de connectivité sécurisée de l'objet connecté depuis le réseau jusqu'à la communication des données qui permet d'appliquer compétences C23 à C30

Production de l'infrastructure réseau et de l'application pour la gestion et la communication es données de l'objet connecté avec la remise d'un prototype et d'un rapport écrit

Evaluation 2 :

Travaux pratiques en équipe qui permettent d'appliquer les compétences C24 à C30

Production de bases de données et de gestion de la technologie cloud computing la remise d'un prototype et rapport écrit

Ces travaux pratiques se réalisent sur des équipements techniques industriels

Evaluation 3 :

Mission en entreprise intégrant une activité de conception ou de déploiement de connectivité sécurisée

Production d'un mémoire suivi d'une présentation orale

RNCP40345BC04 — Réaliser les tests pour un objet connecté sécurisé et robuste pour lancer la phase de pré-industrialisation

LISTE DE COMPÉTENCES

Assurer la veille technologique et réglementaire, en s'assurant que les protocoles et les standards déployés sont bien dans leur dernière mise à jour afin de maintenir une plateforme et un système continuellement à jour pour contrer tous types d'attaques

Définir précisément, le périmètre de la cible de sécurité de l'objet connecté en définissant son contenu et sa structure afin que l'organe de sécurité puisse valider en conséquence

Déterminer les tests d'intrusion adéquats en s'appuyant sur la typologie d'objet connecté et de ses usages afin de déployer la série de tests définie

Déterminer la récurrence de ces tests en prenant en compte les conditions d'usage de l'objet connecté afin de réduire le risque d'attaques

Sensibiliser les utilisateurs en les formant à la politique de cybersécurité afin de développer une culture de la sécurité au sein des organisations

Choisir les tests idoines en prenant en compte les normes vieillissement, de compatibilité électromagnétique, des normes liées aux usages définis par le cahier des charges fonctionnelles afin de réaliser les tests

Valider la robustesse et la fiabilité de l'objet connecté en assurant sa recette et délivrer la certification sécurité afin de passer à la phase d'industrialisation

MODALITÉS D'ÉVALUATION

Evaluation 1 :

Travaux pratiques en équipe qui permettent de définir le périmètre le contenu et la structure de la cible de sécurité qui permettent de mettre en œuvre les compétences de C31 à C37

Production de tests d'intrusion et mise à jour de standards avec la remise d'un scénario et rapport écrit

Ces travaux pratiques se réalisent sur des équipements techniques industriels

Evaluation 2 :

Mission en entreprise intégrant une activité de définition de tests sécurisés et robustes ou de réalisation de tests sécurisés et robustes d'un objet connecté

Production d'un mémoire suivi d'une présentation orale

RNCP40345BC05 — Manager des projets de conception d'un système IoT sécurisé

LISTE DE COMPÉTENCES

Animer l'équipe pluridisciplinaire et multiculturelle en identifiant toutes les expertises techniques et technologiques requises afin de concevoir l'objet connecté sécurisé conforme aux usages attendus

Déployer les outils de conduite de projet en maîtrisant les coûts, la qualité et les délais, de la conception de l'objet connecté afin de répondre au contrat passé avec le client

Manager de manière inclusive les collaborateurs en situation de handicap par exemple, en adaptant les missions des collaborateurs afin qu'ils atteignent les résultats attendus

Etre à l'écoute des problématiques liées aux handicaps en démontrant une action proactive en la matière afin de faciliter l'intégration des collaborateurs

Déployer une stratégie de cybersécurité en formant toutes les parties prenantes internes et externes de l'organisation aux enjeux afin qu'elle soit acceptée et mise en œuvre

Défendre le choix technique et économique de la solution de cybersécurité choisie en en justifiant sa démarche et en démontrant son bénéfice risque afin que les décideurs arrêtent une stratégie financière et commerciale viable pour le déploiement de l'objet connecté

MODALITÉS D'ÉVALUATION

Evaluation 1 :

Etude de cas en groupe sur la conduite de projet technologique innovant en mettant en œuvre les outils et méthodes de management de projet et qui permettent de mettre en œuvre les compétences de C38 à C43

Production : un rapport et une soutenance orale

Evaluation 2 :

Mission en entreprise intégrant une activité de pilotage et management d'un projet d'industrialisation d'un objet connecté

Production d'un mémoire suivi d'une présentation orale

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les entreprises et administrations de toutes tailles, soit des start-ups technologiques, des PME-PMI-ETI et grandes entreprises, et de tous secteurs d'activité sont concernées par ces besoins en expertise. En effet, chaque structure est amenée à anticiper ou gérer les cyberattaques et préserver la confidentialité des données, liées à la conception, la fabrication et/ou l'utilisation de systèmes communicants.

Parmi les secteurs concernés en tout premier lieu, se trouvent des activités à forte valeur ajoutée et capacité d'innovation. De manière non exhaustive : domotique, robotique, télécommunication, énergie, santé, défense, environnement, aéronautique, automobile, nucléaire, commerce, pour ne citer que quelques secteurs.

Cependant selon la taille de la structure concernée et son activité (industrielle, tertiaire), les fonctions mobilisées sont différentes. Par exemple, là où un grand groupe pourra intégrer plusieurs collaborateurs : développeur d'objets connectés, analyste en menaces et incidents de cyber sécurité, chef de projets. D'autres structures de taille plus modeste pourront avoir recours à un consultant en cyber sécurité ou confier ces missions à une personne déjà en poste (Responsable SI).

TYPE D'EMPLOIS ACCESSIBLES

Directeur/Responsable de la sécurité des systèmes communicants

Ingénieur en architecture de réseaux d'IoT

Ingénieur Objet connecté

Objet connecté Designer

Développeur internet d'objets connectés

Ingénieur en Systèmes embarqués

Analyste en menaces et incidents de cyber sécurité

Chercheur en sécurité des systèmes communicants

Intégrateur de solutions de sécurité

Ingénieur R&D

Consultant en cybersécurité

Chef de projet Sécurité

Ingénieur Réseaux

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5)
Facteurs principaux	Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 955 €
Familles professionnelles (FAP)	N0X70 — Techniciens d'étude, recherche et développement · tension 5/5 (Très élevée) N1X90 — Ingénieurs et cadres d'étude, recherche et développement (industrie) · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	15 297
Jugés difficiles à recruter	46 %
Emplois saisonniers	4 %

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :

- Titre d'ingénieur diplômé conférant le grade de master (formations évaluées par la Commission des titres d'ingénieur, liste publiée au journal officiel) ;
- Diplôme d'une école de management, privée ou consulaire, conférant le grade de master (formations évaluées par la CEFDG, liste publiée au bulletin officiel du MESR) ;
- Diplôme de 3ème cycle habilité par les autorités universitaires (Diplôme national de master, DEA, DESS, ...) ou diplôme professionnel de niveau BAC + 5 ;
- Diplôme ou attestation de validation d'un niveau équivalent M1 pour des candidats ayant au moins trois ans d'expérience professionnelle en lien avec la formation visée ;
- Titre inscrit au Répertoire national des certifications professionnelles (RNCP) niveau 7 ;
- Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Ou par la voie de la validation des acquis professionnels et personnels.

Conditions d'accès dérogatoires :

1. Dans la limite de 40 % maximum de l'effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des acquis personnels et professionnels (VAPP), les candidatures de personnes, justifiant a minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation.

2. Par dérogation pour 30 % maximum du nombre d'apprenants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures de titulaires d'un des diplômes suivants :

- Diplôme ou attestation de validation d'un niveau équivalent M1 sans expérience professionnelle ou ayant moins de trois ans d'expérience professionnelle en lien avec la formation visée.
- Diplôme de licence (L3) ou grade de Licence ou titre inscrit au RNCP niveau 6 justifiant d'une expérience professionnelle de 3 ans minimum, en lien avec la formation visée.

Le pourcentage total des dérogation prévues au 1. et 2. ci-dessus ne doit pas excéder 40%.

COMPOSITION DU JURY — FORMATION INITIALE

Le jury est composé de 6 membres

:

- du directeur de Mines Saint-Etienne ou de son représentant dûment habilité
- du responsable pédagogique
- du directeur des partenariats et de l'innovation
- 50% de professionnels externes

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE

Le jury est composé de 6 membres :

- du directeur de Mines Saint-Etienne ou de son représentant dûment habilité
- du responsable pédagogique
- du directeur des partenariats et de l'innovation
- 50% de professionnels externes

COMPOSITION DU JURY — CONTRAT DE PROFESSIONNALISATION, VAE

Le jury est composé au minimum des membres suivants :

- du directeur de Mines Saint-Etienne ou de son représentant dûment habilité
- du responsable pédagogique
- du directeur des partenariats et de l'innovation
- 50% de professionnels externes

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 796 €
Selon la branche	7 700 € – 11 214 €
Prise en charge	Branches concernées
9 796 €	Valeur par défaut · 201 branches
11 214 €	CPNE Travail Temporaire, CPNE des Télécoms, CPNEFP des commerces de gros
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP du Négoce de l'ameublement
11 000 €	CPNE de l'ingénierie, des services informatiques et du conseil
10 000 €	CPNEFP de l'enseignement privé indépendant
9 992 €	CPNEFP Mutualité
9 600 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
9 055 €	CPNEFP Habillement succursaliste
8 500 €	CPNEFP de la métallurgie
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date de décision	28/03/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	28/03/2028
Date de dernière délivrance possible	28/03/2032

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)
RNCP37048

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www.mines-stetienne.fr/formation/mastere-specialise-iot/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40345/>

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1

Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 10/2026 à 09/2028

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).