

Architecte IoT et sécurité des systèmes connectés

RNCP41412 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326m, 326n
Formacode(s)	31023, 31042
Code(s) ROME	M1805, M1806, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/10/2025
Date d'échéance	27/10/2028

Certificateur(s)

QUEST EDUCATION GROUP · SIRET : 83767023100021

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
GAZELGROUP	92787773800017	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100021	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100047	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100054	Former et organiser l'évaluation
QUEST EDUCATION GROUP	83767023100062	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification « Architecte IoT et sécurité des systèmes connectés » vise à former des professionnels capables de concevoir, piloter et sécuriser des infrastructures IoT dans des environnements complexes. Le contexte actuel, marqué par la transformation numérique et la prolifération des objets connectés, requiert des experts maîtrisant les enjeux technologiques, réglementaires et éthiques. Cette certification de niveau 7 répond aux besoins croissants des entreprises dans un secteur en tension, en dotant les titulaires de compétences indispensables pour garantir la sécurité, l'intégrité et la conformité des systèmes connectés.

ACTIVITÉS VISÉES

L'Architecte IoT et sécurité des systèmes connectés assure des responsabilités variées allant de l'analyse des besoins, la conception et la sécurisation des infrastructures IoT, à la maintenance et l'accompagnement au changement dans un environnement en constante évolution. Ces activités incluent notamment :

ACTIVITÉ 1 - Cadrage et analyse d'un projet IoT intégrant les technologies émergentes et la cybersécurité

ACTIVITÉ 2 - Conception et modélisation de l'architecture d'un projet IoT (programmes, infrastructures, réseaux sécurisés)

ACTIVITÉ 3 - Pilotage et accompagnement du déploiement opérationnel d'un projet IoT sécurisé

ACTIVITÉ 4 - Intégration, sécurisation et mise en conformité des systèmes IoT connectés

ACTIVITÉ 5 - Maintenance et évolution des systèmes connectés sécurisés en condition opérationnelle

COMPÉTENCES ATTESTÉES

Analyser les besoins métier et les contraintes organisationnelles d'un projet IoT, en identifiant les objectifs stratégiques et opérationnels, afin de définir les composantes techniques et fonctionnelles de la solution.

Évaluer les contraintes réglementaires, les risques en matière de cybersécurité et de protection des données dès la phase amont, afin de garantir une approche security & privacy by design conforme aux exigences légales, normatives et éthiques.

Formaliser une note de cadrage et un cahier des charges fonctionnel intégrant les objectifs, périmètre, contraintes organisationnelles, réglementaires et de cybersécurité, ainsi que les exigences des parties prenantes, afin de garantir la clarté et l'alignement du projet.

Identifier et cartographier les parties prenantes ainsi que les systèmes existants, en analysant les vulnérabilités et points de compatibilité, afin de préparer l'intégration future de la solution IoT.

Réaliser une étude de faisabilité technico-économique en analysant les aspects techniques, opérationnels et budgétaires, afin de déterminer la viabilité du projet et justifier la cohérence des choix auprès du commanditaire.

Évaluer les impacts environnementaux liés à la conception d'une solution IoT (consommation énergétique, cycle de vie des équipements, empreinte écologique), afin de proposer des solutions écoresponsables conformes aux engagements de durabilité

Identifier les innovations technologiques, réglementaires et environnementales en mobilisant les résultats de la veille prospective nationale et internationale réalisée sur les tendances sectorielles et les menaces émergentes, afin de positionner le projet dans une perspective durable, compétitive et sécurisée.

Concevoir des architectures techniques et fonctionnelles IoT intégrant les contraintes de cybersécurité, de performance, de scalabilité et d'interopérabilité, afin de garantir la robustesse et l'évolutivité de la solution.

Modéliser les interactions entre les différentes couches de l'architecture IoT (physique, réseau, logicielle, applicative), afin d'assurer une intégration cohérente et sécurisée.

Intégrer des standards et technologies favorisant l'accessibilité universelle, y compris l'accessibilité numérique (RGAA, WCAG), dans les conceptions fonctionnelles et techniques, afin d'assurer l'inclusivité des systèmes connectés.

Définir une architecture de données adaptée aux besoins métiers et techniques, en qualifiant, structurant et hiérarchisant les données collectées, afin d'en assurer la fiabilité et la pertinence.

Concevoir les flux de données et les mécanismes de traitement, en intégrant des processus d'automatisation, de sécurisation et de sobriété énergétique afin d'optimiser la circulation, la durabilité et l'exploitation des informations

Prévoir et intégrer l'usage de solutions d'intelligence artificielle et de machine learning dans les processus IoT, en identifiant les cas d'usage pertinents et en garantissant leur interopérabilité, afin de renforcer la performance, la sécurité et la valeur ajoutée de l'architecture.

Concevoir et développer des prototypes et maquettes IoT en intégrant les composants matériels, logiciels et réseaux, et en veillant à l'accessibilité et à l'inclusivité des usages, afin de valider la faisabilité, la robustesse et l'universalité de la solution.

Configurer et paramétrer les plateformes IoT et applications associées, afin de tester leur compatibilité avec les besoins fonctionnels et sécuritaires.

Adapter les logiciels métier et applicatifs aux besoins spécifiques de la plateforme IoT, afin de garantir leur intégration et leur performance.

Piloter la gestion opérationnelle d'un projet IoT en estimant et en suivant le budget, en définissant et en allouant les ressources humaines et matérielles, et en planifiant les étapes, afin de garantir la maîtrise des coûts et la disponibilité des moyens nécessaires au déploiement.

Superviser et contrôler le cahier des charges technique, en intégrant les exigences de cybersécurité, réglementaires et opérationnelles, afin de garantir la conformité du déploiement du projet.

Contrôler la cohérence des spécifications et leur adéquation avec les besoins exprimés par les parties prenantes, afin d'assurer la qualité et la fiabilité du projet IoT.

Coordonner les équipes internes et externes impliquées dans un projet IoT, en animant la collaboration pluridisciplinaire selon des méthodes de pilotage adaptées (agiles ou hybrides), et en synchronisant les contributions, afin de garantir la cohérence du déploiement et l'alignement du projet avec les objectifs stratégiques.

Accompagner les utilisateurs dans l'adoption de la solution IoT en concevant et déployant des actions de formation et

de communication couvrant les usages métier, l'accessibilité numérique (RGAA, WCAG), la protection des données et la cybersécurité, afin de favoriser une appropriation durable, inclusive et sécurisée.

Intégrer une solution IoT dans un système d'information en configurant les paramètres techniques, en validant la compatibilité et en ajustant les éléments issus du prototypage, afin de garantir l'interopérabilité et la continuité opérationnelle

Contrôler et valider les flux de données et les performances de la solution IoT au moyen de tests d'intégrité, de fiabilité et de connectivité, afin d'assurer la robustesse et la conformité du système.

Identifier et analyser les vulnérabilités potentielles des composants IoT (physiques, réseaux, logiciels), afin de concevoir des mesures correctives et de définir les priorités de sécurisation.

Déployer et superviser des mécanismes de sécurisation (IAM, chiffrement, authentification forte, supervision des infrastructures), afin de protéger les systèmes IoT contre les intrusions et les usages non autorisés.

Réaliser des tests de sécurité (vérification des mécanismes de protection, simulation de cyberattaques, scénarios d'accessibilité), afin d'évaluer la résilience et la capacité de défense de la solution IoT

Réaliser des audits de conformité réglementaire et normative (RGPD, NIS2, ISO, etc.), afin de garantir l'adéquation des systèmes IoT aux exigences légales et sectorielles.

Élaborer des rapports d'audit et formuler des recommandations de mise en conformité, afin d'orienter les décisions stratégiques et opérationnelles.

Définir et actualiser une stratégie de gestion des risques IoT, en identifiant les menaces et en proposant des plans de mitigation, afin d'assurer la sécurité et la résilience du système.

Détecter et analyser les incidents de sécurité IoT à l'aide d'outils spécialisés (SIEM, IDS...), afin d'identifier rapidement les anomalies et les intrusions.

Coordonner et mettre en œuvre les actions correctives suite à un incident de sécurité, afin de rétablir la continuité opérationnelle et de limiter les impacts.

Produire des rapports post-incident et formuler des recommandations d'amélioration continue, en intégrant des retours d'expérience (RETEX) et des enseignements opérationnels, afin de renforcer la résilience des systèmes connectés et d'anticiper les menaces futures.

Définir et mettre en œuvre un plan de maintenance préventive et corrective, en identifiant les éléments critiques à surveiller, afin de garantir la disponibilité et la performance des systèmes connectés.

Suivre et analyser les indicateurs de performance technique des systèmes IoT, afin de détecter les anomalies et de déclencher les actions correctives adaptées.

Coordonner les interventions de maintenance corrective, préventive et prédictive en lien avec les équipes internes et prestataires, afin d'assurer la continuité opérationnelle et d'anticiper les défaillances critiques.

Produire et actualiser la documentation technique relative aux systèmes IoT (procédures, configurations, consignes de sécurité), en veillant à son accessibilité pour tous les utilisateurs, afin d'assurer leur traçabilité et leur exploitation.

Organiser et superviser le support technique et le transfert de compétences auprès des équipes et des utilisateurs, en structurant les dispositifs d'assistance et en garantissant leur réactivité, afin d'assurer la continuité d'utilisation et l'autonomie des acteurs impliqués.

Élaborer et justifier des stratégies d'évolution et d'adaptation des solutions IoT, en intégrant des évolutions techniques (IA, blockchain, sobriété numérique, protocoles sécurisés) et en tenant compte des usages émergents, des contraintes réglementaires et environnementales, afin d'améliorer la résilience, la sécurité et la durabilité des systèmes connectés.

Gérer le cycle de vie des équipements IoT en planifiant leur remplacement, leur mise hors service et leur recyclage, afin de garantir la continuité opérationnelle et de respecter les exigences de durabilité et de conformité environnementale.

Blocs de compétences

RNCP41412BC01 — Cadrer et analyser un projet IoT intégrant les technologies émergentes et la cybersécurité

LISTE DE COMPÉTENCES

Analyser les besoins métier et les contraintes organisationnelles d'un projet IoT, en identifiant les objectifs stratégiques et opérationnels,

Évaluer les contraintes réglementaires, les risques en matière de cybersécurité et de protection des données dès la phase amont,

Formaliser une note de cadrage et un cahier des charges fonctionnel intégrant les objectifs, périmètre, contraintes organisationnelles, réglementaires et de cybersécurité, ainsi que les exigences des parties prenantes,
Identifier et cartographier les parties prenantes ainsi que les systèmes existants, en analysant les vulnérabilités et points de compatibilité,
Réaliser une étude de faisabilité technico-économique en analysant les aspects techniques, opérationnels et budgétaires,
Évaluer les impacts environnementaux liés à la conception d'une solution IoT (consommation énergétique, cycle de vie des équipements, empreinte écologique),
Identifier les innovations technologiques, réglementaires et environnementales en mobilisant les résultats de la veille prospective nationale et internationale réalisée sur les tendances sectorielles et les menaces émergentes.

MODALITÉS D'ÉVALUATION

Étude de cas avec mise en situation professionnelle simulée : écrit

RNCP41412BC02 — Concevoir et modéliser l'architecture d'un projet IoT (programmes, infrastructures, réseaux sécurisés)

LISTE DE COMPÉTENCES

Concevoir des architectures techniques et fonctionnelles IoT intégrant les contraintes de cybersécurité, de performance, de scalabilité et d'interopérabilité,
Modéliser les interactions entre les différentes couches de l'architecture IoT (physique, réseau, logicielle, applicative),
Intégrer des standards et technologies favorisant l'accessibilité universelle, y compris l'accessibilité numérique (RGAA, WCAG), dans les conceptions fonctionnelles et techniques,
Définir une architecture de données adaptée aux besoins métiers et techniques, en qualifiant, structurant et hiérarchisant les données collectées,
Concevoir les flux de données et les mécanismes de traitement, en intégrant des processus d'automatisation, de sécurisation et de sobriété énergétique
Prévoir et intégrer l'usage de solutions d'intelligence artificielle et de machine learning dans les processus IoT, en identifiant les cas d'usage pertinents et en garantissant leur interopérabilité,
Concevoir et développer des prototypes et maquettes IoT en intégrant les composants matériels, logiciels et réseaux, et en veillant à l'accessibilité et à l'inclusivité des usages,
Configurer et paramétrer les plateformes IoT et applications associées, afin de tester leur compatibilité avec les besoins fonctionnels et sécuritaires.
Adapter les logiciels métier et applicatifs aux besoins spécifiques de la plateforme IoT.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée : écrit

RNCP41412BC03 — Piloter et accompagner le déploiement opérationnel d'un projet IoT sécurisé

LISTE DE COMPÉTENCES

Piloter la gestion opérationnelle d'un projet IoT en estimant et en suivant le budget, en définissant et en allouant les ressources humaines et matérielles, et en planifiant les étapes,
Superviser et contrôler le cahier des charges technique, en intégrant les exigences de cybersécurité, réglementaires et opérationnelles,
Contrôler la cohérence des spécifications et leur adéquation avec les besoins exprimés par les parties prenantes,
Coordonner les équipes internes et externes impliquées dans un projet IoT, en animant la collaboration pluridisciplinaire selon des méthodes de pilotage adaptées (agiles ou hybrides), et en synchronisant les contributions,
Accompagner les utilisateurs dans l'adoption de la solution IoT en concevant et déployant des actions de formation et de communication couvrant les usages métier, l'accessibilité numérique (RGAA, WCAG), la protection des données et la cybersécurité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée : soutenance orale de projet

RNCP41412BC04 — Intégrer, sécuriser et mettre en conformité des systèmes IoT connectés

LISTE DE COMPÉTENCES

Intégrer une solution IoT dans un système d'information en configurant les paramètres techniques, en validant la compatibilité et en ajustant les éléments issus du prototype,
Contrôler et valider les flux de données et les performances de la solution IoT au moyen de tests d'intégrité, de

fiabilité et de connectivité,

Identifier et analyser les vulnérabilités potentielles des composants IoT (physiques, réseaux, logiciels),

Déployer et superviser des mécanismes de sécurisation (IAM, chiffrement, authentification forte, supervision des infrastructures),

Réaliser des tests de sécurité (vérification des mécanismes de protection, simulation de cyberattaques, scénarios d'accessibilité),

Réaliser des audits de conformité réglementaire et normative (RGPD, NIS2, ISO, etc.),

Élaborer des rapports d'audit et formuler des recommandations de mise en conformité,

Définir et actualiser une stratégie de gestion des risques IoT, en identifiant les menaces et en proposant des plans de mitigation,

Détecter et analyser les incidents de sécurité IoT à l'aide d'outils spécialisés (SIEM, IDS...),

Coordonner et mettre en œuvre les actions correctives suite à un incident de sécurité,

Produire des rapports post-incident et formuler des recommandations d'amélioration continue, en intégrant des retours d'expérience (RETEX) et des enseignements opérationnels.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée : étude de cas technique

RNCP41412BC05 — Maintenir et faire évoluer des systèmes connectés sécurisés en condition opérationnelle

LISTE DE COMPÉTENCES

Définir et mettre en œuvre un plan de maintenance préventive et corrective, en identifiant les éléments critiques à surveiller,

Suivre et analyser les indicateurs de performance technique des systèmes IoT,

Coordonner les interventions de maintenance corrective, préventive et prédictive en lien avec les équipes internes et prestataires,

Produire et actualiser la documentation technique relative aux systèmes IoT (procédures, configurations, consignes de sécurité), en veillant à son accessibilité pour tous les utilisateurs,

Organiser et superviser le support technique et le transfert de compétences auprès des équipes et des utilisateurs, en structurant les dispositifs d'assistance et en garantissant leur réactivité,

Élaborer et justifier des stratégies d'évolution et d'adaptation des solutions IoT, en intégrant des évolutions techniques (IA, blockchain, sobriété numérique, protocoles sécurisés) et en tenant compte des usages émergents, des contraintes réglementaires et environnementales,

Gérer le cycle de vie des équipements IoT en planifiant leur remplacement, leur mise hors service et leur recyclage.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle pratique – Etude et présentation orale d'un cas pratique

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le métier d'Architecte IoT et Sécurité des Systèmes Connectés s'exerce dans divers contextes professionnels, adaptés aux spécificités de chaque organisation et projet. Voici quelques exemples représentatifs :

Dans une grande entreprise ou un groupe international : L'Architecte IoT peut intégrer une direction technique ou un département spécialisé en systèmes connectés et cybersécurité. Son rôle consiste à concevoir des architectures IoT à grande échelle, sécuriser les infrastructures critiques, et piloter des projets innovants en collaboration avec des équipes pluridisciplinaires, incluant des spécialistes des données et des développeurs.

Dans une PME ou une startup spécialisée dans l'IoT : L'Architecte IoT joue un rôle central et polyvalent, assumant à la fois la conception stratégique et l'exécution opérationnelle des projets IoT. Il peut contribuer à définir la vision technologique de l'entreprise, intégrer des solutions innovantes, et répondre aux besoins spécifiques des secteurs comme la santé, les villes intelligentes ou l'industrie.

En tant que consultant IoT et cybersécurité : Travaillant de manière indépendante ou pour des cabinets de conseil, l'Architecte IoT intervient auprès de diverses entreprises pour auditer, concevoir et sécuriser des solutions IoT adaptées à leurs besoins. Ce rôle requiert une expertise approfondie en cybersécurité et une capacité à s'adapter rapidement à des environnements variés.

Dans des organismes publics ou parapublics : L'Architecte IoT contribue à des projets d'intérêt général, comme la

sécurisation des infrastructures connectées dans les domaines de la défense, des transports, ou des collectivités locales. Ces missions impliquent souvent une collaboration étroite avec des partenaires institutionnels et une prise en compte rigoureuse des contraintes réglementaires.

Dans les secteurs industriels spécialisés : Les entreprises de l'Industrie 4.0, les fournisseurs d'énergie, et les acteurs du transport et de la logistique emploient des Architectes IoT pour superviser la mise en place de systèmes connectés complexes, sécuriser les chaînes de production et d'approvisionnement, et optimiser les processus via des technologies comme l'IA et le big data.

TYPE D'EMPLOIS ACCESSIBLES

- Architecte IoT
- Expert en infrastructures connectées
- Développeur Internet des Objets
- Ingénieur Internet des Objets
- Concepteur de solutions IoT (Internet of Things)
- Ingénieur systèmes embarqués connectés
- Consultant IoT et cybersécurité
- Chef de projet en cybersécurité IoT

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier d'Architecte IoT et Sécurité des Systèmes Connectés n'est pas directement réglementé. Cependant, il est soumis à des cadres législatifs et normatifs liés à la protection des données personnelles (RGPD), à la cybersécurité (Directive NIS2), ainsi qu'à des réglementations spécifiques dans des secteurs sensibles tels que la santé ou les infrastructures critiques. Les normes internationales, telles que l'ISO 27001 pour la gestion de la sécurité de l'information, jouent également un rôle clé. Ces exigences sont intégrées dans le référentiel de compétences et d'évaluation pour garantir une conformité aux obligations légales et normatives.

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) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	32 216
Jugés difficiles à recruter	51 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour l'entrée en formation :

- Être titulaire d'un titre de niveau 6 dans un domaine en lien avec l'ingénierie numérique
- Sélection sur dossier et entretien de motivation

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury de délivrance de la certification est composé de 4 membres dont :

- 3 professionnels externes à l'organisme certificateur, possédant une expertise reconnue dans les domaines IoT et/ou cybersécurité
- 1 membre interne à l'organisme certificateur (directeur national de la pédagogie ou son représentant)

Base légale

Date de décision	27/10/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/10/2028
Date de dernière délivrance possible	26/10/2032

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP38906, RNCP38920

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41412/>