

Ingénieur spécialisé en sécurité pour les systèmes informatiques et les communications, diplômé d'EURECOM

RNCP39907 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	110, 326, 326m
Formacode(s)	31006, 24293, 32062, 15099
Code(s) ROME	M1802, M1803, M1806, M1804, M1805
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2028

Certificateur(s)

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE · SIRET : 11004401300040
EURECOM · SIRET : 38318157500028

Résumé de la certification

OBJECTIFS ET CONTEXTE

Cette certification répond à un besoin d'ingénieurs spécialisés dans les domaines de la sécurité numérique, qui maîtrisent les différents aspects de la sécurité numérique :

- Sécurité logicielle
- Sécurité matérielle
- Sécurité des communications et des réseaux
- Sécurité des objets connectés
- Sécurité des appareils mobiles
- Sécurité physique (reconnaissance faciale, biométrie)
- Forensique

Ce besoin d'ingénieurs est identifié dans la plupart des secteurs d'activité, que ce soit auprès des entreprises de toutes tailles ou des administrations publiques, et cette certification ouvre de très bonnes perspectives d'emploi dans des secteurs d'activités très variés.

La certification d'ingénieur spécialisé vise à apporter un ensemble de compétences spécifiques à la sécurité numérique. à un public d'ingénieurs diplômés maîtrisant déjà un large socle de compétences.

ACTIVITÉS VISÉES

L'ingénieur de spécialisation, diplômé d'EURECOM en sécurité pour les systèmes informatiques et les communications à travailler à la définition, la conception, le développement, la déploiement et à la mise en oeuvre des solutions de sécurité numérique au sens large.

De façon non exhaustive, cela couvre les activités suivantes :

- Gestion de la sécurité informatique globale d'une entreprise
- Pilotage d'un projet complexe dans un environnement multiculturel
- Conception et réalisation d'un système numérique sécurisé
- Activité de recherche incluant des interactions scientifiques avec des pairs
- Analyse des menaces actuelles et futures d'un système et d'un réseau informatique existants

- Conception et mise en œuvre de systèmes d'informations et de réseaux sécurisés
- Participation à des instances qui régissent la protection de la vie privée dans les systèmes informatiques et les réseaux

COMPÉTENCES ATTESTÉES

La certification d'ingénieur spécialisé en sécurité pour les systèmes informatiques et les communications d'EURECOM doit permettre de valider les compétences d'un ingénieur en sciences du numérique spécialisé en sécurité, ce qui implique durant le cursus l'acquisition des connaissances, savoir-faire, savoir-être et aptitudes nécessaires à leur développement :

- connaître et comprendre un large champ des sciences du numériques et des mathématique et analyser et réaliser la synthèse qui leur est associée
- mobiliser les ressources d'un ou de plusieurs champ scientifique et technique spécifique
- maîtriser les méthodes et les outils de l'ingénieur, l'utilisation des approches numériques et des outils informatiques, l'analyse, la modélisation et la conception de systèmes numériques ou de communication, de produit ou de service, la gestion des risques et des crises, la pratique du travail collaboratif et à distance
- concevoir, concrétiser, tester et valider des solutions, des méthodes, produits, systèmes et services innovants, en ayant préalablement un questionnement sur les usages
- effectuer des activités de recherche, fondamentale ou appliquée, mettre en place des dispositifs expérimentaux
- trouver l'information pertinente, l'évaluer et l'exploiter, et transmettre son savoir à travers des publications ou des conférences
- prendre en compte les enjeux de l'entreprise et rendre compte de son action : dimension économique, respect des exigences sociales et environnementales, respect de la qualité, compétitivité et productivité, exigences commerciales, intelligence économique
- intégrer dans ses conduites les responsabilités éthiques et professionnelles, prendre en compte les enjeux des relations au travail, de sécurité et de santé au travail et de la diversité
- accompagner les transitions, notamment numériques, énergétiques et environnementales, en intégrant les impératifs écologiques et climatiques
- prendre en compte les enjeux et les besoins de la société et diffuser les principes et apports de la démarche scientifique
- s'insérer dans la vie professionnelle, s'intégrer dans une organisation internationale, l'animer et la faire évoluer
- entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux
- travailler en contexte international et multiculturel : maîtrise d'une ou plusieurs langues étrangères et ouverture culturelle associée, capacité d'adaptation aux contextes internationaux et de coopération sur des enjeux planétaires collectifs
- se connaître, s'autoévaluer, gérer ses compétences et opérer des choix professionnel
- définir l'architecture d'un système de communication sécurisé
- concevoir les composantes d'un système de communication sécurisé
- concevoir des composantes logicielles résistants aux attaques informatiques
- concevoir les mécanismes de sécurité destinés à un système informatique
- réaliser un prototype logiciel pour un système informatique sécurisé
- concevoir de nouveaux algorithmes pour la sécurité des systèmes informatiques
- mettre en œuvre le plan directeur d'un réseau sécurisé
- évaluer les performances de solutions de sécurité existante
- mener une campagne d'audit de sécurité pour un réseau d'entreprise ou un système d'information
- assurer la gestion de la sécurité informatique au sein d'une entreprise
- mener une campagne d'audit de sécurité pour un réseau d'entreprise ou un système d'information
- participer aux travaux de normalisation dans le domaine de la sécurité informatique et réseaux

Blocs de compétences

RNCP39907BC01 — S'adapter aux enjeux propres de l'entreprise en prenant en compte la dimension organisationnelle, personnelle et culturelle

LISTE DE COMPÉTENCES

- Analyser la complexité d'un projet de sécurité informatique dans sa mise en œuvre en identifiant l'ensemble des

implications afin de répondre au cahier des charges

- Assurer la gestion de la sécurité informatique au sein d'une entreprise en respectant les règles d'éthique afin de garantir la confidentialité des données
- Interagir dans un environnement international par l'acquisition de compétences interculturelles et l'usage d'une ou plusieurs langue(s) étrangère(s) afin de communiquer efficacement et respectueusement au sein d'équipes multiculturelles
- Piloter des ressources internationales liées à un projet ou à une affaire en utilisant des outils de travail collaboratif afin d'assurer une cohérence dans le travail d'équipe, y compris pour des membres en situation de handicap

MODALITÉS D'ÉVALUATION

- Etude de cas sur l'analyse d'un projet de sécurité informatique à partir d'un cahier des charges
- Mise en situation dans le cadre de challenge ou projets – Production d'un Poster en anglais et soutenance de la production de manière collective
- Epreuves écrites

RNCP39907BC02 — Définir, concevoir et implémenter des outils et méthodes innovants dans les domaines de la sécurité informatique avec une approche basée sur la recherche scientifique

LISTE DE COMPÉTENCES

- Définir l'architecture d'un système de communication sécurisé en utilisant les outils mathématiques et informatiques appropriés afin de garantir l'intégrité et la confidentialité des données
- Développer un prototype logiciel des composants d'un système informatique sécurisé en intégrant les outils de protection appropriés afin d'éviter les intrusions numériques malveillantes
- Mettre en œuvre les outils cryptographiques en respectant des protocoles et les dernières avancées de l'état de l'art pour sécuriser les communications et les données
- Concevoir une ébauche d'article de recherche en vue de le présenter oralement en anglais selon le formalisme dicté par les revues scientifiques de recherche dans le domaine du numérique
- Réaliser une veille scientifique sur des domaines techniques et sociologiques en menant une activité de recherche et d'analyse d'informations afin de pouvoir proposer les solutions les plus innovantes

MODALITÉS D'ÉVALUATION

- Mise en situation dans le cadre de projets ou challenges
- Réalisation d'une ébauche d'article et soutenance en anglais
- Rapport rédigé en anglais sur l'analyse bibliographique réalisée

RNCP39907BC03 — Concevoir et mettre en œuvre les systèmes globaux de sécurité informatique et de protection des données et des communications

LISTE DE COMPÉTENCES

- Identifier les menaces d'un système existant en utilisant les détecteurs les plus efficaces afin de proposer des parades
- Mesurer l'impact de l'utilisation malveillante d'un système numérique en utilisant des détecteurs appropriés afin de mettre en place une stratégie de sécurité numérique adaptée
- Concevoir les composantes logicielles résistants aux attaques informatiques en utilisant de nouveaux algorithmes pour la sécurité des systèmes informatiques afin de sécuriser des systèmes numériques ou cyber-physiques et de garantir l'intégrité et la confidentialité des données
- Mettre en œuvre le plan directeur d'un système d'information ou d'un réseau sécurisé en prenant en compte les usages et en minimisant l'impact énergétique afin que la gestion des données de l'entreprise soit opérationnelle et sécurisée

MODALITÉS D'ÉVALUATION

- Mise en situation dans le cadre de projets ou challenges
- Réalisation d'un projet

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Centres de Recherche et Développement
- Opérateurs de téléphonie mobile

- Sociétés de Conseil en Sécurité, Informatique et Réseaux
- Opérateurs de Systèmes de Communication
- Industriels fournisseurs de technologies pour les systèmes informatiques ou de communications
- Secteur tertiaire mettant en œuvre des transactions sécurisées (banques, assurances, ...)
- Administrations publiques, hôpitaux
- Département Systèmes d'Informations d'entreprises, quel que soit le secteur d'activité
- Organismes de standardisation dans le domaine de la sécurité numérique

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur Recherche et Développement
- Architecte de solutions
- Ingénieur Cybersécurité
- Consultant
- Chef de projet cybersécurité
- Ingénieur d'affaires
- Créateur d'entreprise

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)	2 892 €
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) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre diplômés d'un titre d'ingénieur du niveau 7, délivré par une école française accréditée par la CTI.

Le recrutement peut être étendu à certains titulaires d'un diplôme d'ingénieur étranger ou d'un grade de master en ingénierie étranger. Sont inclus automatiquement dans cette catégorie les formations ayant reçu une admission par l'Etat à la suite d'un audit de la CTI et les formations ayant obtenu le label EUR-ACE® (European Accredited Engineer) par une agence autorisée par ENAEE.

Exceptionnellement, l'école peut admettre des candidats étrangers issus d'autres formations, mais doit toutefois être en mesure de justifier, a posteriori, la qualité de ces formations étrangères retenues. L'analyse de recevabilité se base sur l'étude des caractéristiques de la formation et du diplôme et non sur le dossier de l'élève.

COMPOSITION DU JURY — FORMATION INITIALE

Jury constitué des membres suivants :

- Directeur de l'établissement
- Directeur des Etudes
- Responsable du service scolarité
- Le professeur responsable de la formation
- Un professeur représentant l'ensemble du corps professoral
- Un membre externe, représentant l'Institut Mines-Télécom

COMPOSITION DU JURY — FORMATION CONTINUE

Jury constitué des membres suivants :

- Directeur de l'établissement
- Directeur des études
- Le professeur responsable de la formation
- Un professeur représentant l'ensemble du corps professoral
- Responsable du service scolarité
- Un membre externe, représentant l'Institut Mines-Télécom

COMPOSITION DU JURY — VAE

Jury constitué des membres suivants :

- Directeur de l'établissement
- Directeur des études
- Le professeur responsable de la formation
- Un professeur représentant l'ensemble du corps professoral
- Responsable du service scolarité
- 2 représentants du secteur professionnel considéré, qui ne soient pas membres de l'entreprise du candidat.

Base légale

Date d'échéance de l'enregistrement	31/08/2028
-------------------------------------	------------

Date de dernière délivrance possible	31/08/2031
--------------------------------------	------------

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP16400

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.eurecom.fr/fr/les-formations/ingenieur-specialise/ingenieur-en-securite-des-systemes-informatiques-et>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39907/>