Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 23515**

Intitulé

MASTER : MASTER Science Technologies Santé, mention Réseaux et Télécommunication

AUTORITÉ RESPONSABLE DE LA CERTIFICATION

Ministère de l'Enseignement Supérieur, Université de Valenciennes et du Hainaut-Cambrésis

QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION

Recteur de l'Académie, Président de l'Université

Niveau et/ou domaine d'activité

I (Nomenclature de 1967)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

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

Formacode(s) :

24252 réseau télécom, 31006 sécurité informatique

Résumé du référentiel d'emploi ou éléments de compétence acquis

Les professionnels ayant suivi ce parcours type Cyber-défense et sécurité de l'information, auront pour mission principale de **lutter contre la cybercriminalité et les failles des systèmes d'information**. Ils traiteront les problèmes liés aux domaines de la **sécurité numérique** et du **codage de l'information** afin de pouvoir assurer la disponibilité des services, la confidentialité des informations et l'authentification des contenus informatiques. Grâce à leurs compétences dans le domaine de la connectivité intelligente entre objets ou machines (Paiement à distance, domotique, montres connectées...) et leurs connaissances des techniques de liaison sans fil (RFID, NFC...) ils pourront répondre aux vulnérabilités de ces systèmes, aux cyber-attaques. Ils pourront aussi améliorer la sécurité de l'utilisation de ces objets connectés dans le domaine de la santé. Ils pourront également traiter des problématiques spécifiques de la sécurité des systèmes de transport intelligents (Communication inter-véhicules, véhicule-infrastructure...).

- Assurer la sécurité d'un système informatique en connaissant les techniques de hacking, les menaces et les failles des applications et systèmes actuels.

- Réaliser des audits de l'informatique industrielle et de gestion notamment sur la base des normes européennes de sécurité.

- Assurer la sécurité des procédés industriels.

- Concevoir et analyser des cryptosystèmes et des codes en vue d'application dans la sécurité de l'information.

- Mettre en œuvre ses compétences dans le domaine émergent de la radio intelligente pour la sécurité de l'information.

- Assurer l'ouverture vers des nouvelles technologies sécurisées en étudiant les architectures et les déploiements des réseaux de capteurs.

- Assurer la sécurité des contenus multimédia, des communications mobiles, des bases de données et du Cloud

- Assurer la sécurité des systèmes embarqués en étudiant leurs mécanismes

- Etudier les principes des systèmes de transport intelligents et pour assurer leurs sécurités.

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

Ces professionnels pourront exercer dans l'ensemble des secteurs où la défense et la sécurité de l'information sont au cœur de l'activité.

On peut citer notamment les secteurs :

Transports

Informatique

Réseaux

Services

Responsable de la sécurité du système d'information

Auditeur en sécurité des systèmes d'information,

Evaluateur d'applications sécurisées.

Ingénieur d'études et développement de logiciels sécurisés

Consultant en sécurité de l'information

Auditeur technique ou organisationnel, intégrateur

Architecte sécurité (informatique et télécom)

Administrateur de la sécurité (informatique et télécom)

Enseignant-Chercheur en sécurité informatique et électronique (après un doctorat)

Codes des fiches ROME les plus proches :

H1206 : Management et ingénierie études, recherche et développement industriel

M1801 : Administration de systèmes d'information

M1802 : Expertise et support en systèmes d'information

M1803 : Direction des systèmes d'information

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

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

L'inscription en M1 est ouverte aux étudiants titulaires d'une licence informatique, mathématiques appliquées, GEII/EEA ou une licence systèmes d'information et réseaux. Les meilleurs étudiants titulaires d'une licence professionnelle « réseaux et télécom ou CDAISI » peuvent intégrer le Master 1 via une validation (VAP 85) sur la base d'un dossier de candidature et d'entretien prouvant leur motivation.

Les étudiants venant d'universités étrangères et titulaires d'une licence équivalente (ou tout autre diplôme de même niveau, équivalent) peuvent être admis après l'examen de leurs dossiers de candidature ainsi que les entretiens de motivation.

Les étudiants ayant obtenu les 60 crédits ECTS du master 1 CDSI peuvent intégrer directement la deuxième année de master. Toutefois, une nouvelle campagne de recrutement est ouverte aux étudiants ayant validé leurs master 1 informatique, mathématiques appliquées, réseaux et télécoms, système d'information et réseaux.

Les élèves ingénieurs en dernière année ainsi que les étudiants étrangers ayant validé un diplôme équivalent peuvent également intégrer l'année M2 après avoir candidaté sur dossier.

Liste des modules :

M1-S7 :

- Remise à niveau réseaux et télécommunication - 3 ECTS, 34 heures
- Outils mathématiques pour le codage et la sécurité de l'information- 3 ECTS, 32 heures
- Algèbre et théorie des nombres pour la cryptographie - 3 ECTS, 32 heures
- Techniques de Hacking et failles des systèmes - 4 ECTS, 32 heures
- Programmation distribuée et sécurité- 4 ECTS, 32 heures
- Sécurité des objets mobiles communicants- 4 ECTS, 32 heures
- Bases des données et internet- 3 ECTS, 32 heures
- Anglais- 3 ECTS, 36 heures
- comportement humain et faille des systèmes- 1,5 ECTS, 18 heures
- Aspect juridique - 1,5 ECTS, 18 heures

M1-S8 :

- Cryptographie et codes correcteurs d'erreurs - 3 ECTS, 32 heures
- Complexité des algorithmes - 3 ECTS, 32 heures
- Normes de sécurité, Audits et analyse des risques (EBIOS...) - 3 ECTS, 32 heures
- Réseaux de capteurs - 3 ECTS, 32 heures
- Sécurité des systèmes embarqués - 3 ECTS, 32 heures
- Sécurité des contenus multimédia et codage - 3 ECTS, 32 heures
- Plateaux projet (en relation avec les entreprises) - 6 ECTS, 24 heures
- Anglais - 3 ECTS, 36 heures
- SHS 1 COMM - 1,5 ECTS, 18 heures
- SHS 2 gestion Projet - 1,5 ECTS, 18 heures

M2-S9 :

- Cryptographie avancée - 3 ECTS, 32 heures
- Cyber-sécurité - 4 ECTS, 32 heures
- Privacité et sécurité des données - 3 ECTS, 32 heures
- Sécurité des accès distants - 3 ECTS, 32 heures
- Systèmes de transport intelligents - 4 ECTS, 32 heures
- Sécurité de la radio intelligente et USRP - 3 ECTS, 32 heures
- Sécurité informatique des procédés industriels - 4 ECTS, 32 heures
- Anglais - 3 ECTS, 32 heures
- Média training - 1,5 ECTS, 18 heures
- SHS : Insertion professionnelle - 1,5 ECTS, 18 heures

M2-S10 :

- Plateaux projet (en relation avec les entreprises) - 6 ECTS, 36 heures
- STAGE 6 mois - 24 ECTS

Les modalités de contrôle des connaissances:

Chaque unité d'enseignement donne lieu à une évaluation selon des modalités propres à chacune d'elle : contrôle classique de connaissances, mini projet, mémoire et soutenance (stage, projet)... Chaque évaluation conduit à une notation. Les différentes évaluations au sein d'une unité d'enseignement sont pondérées en fonction de leur importance pour donner la note finale de l'UE.

Si la note de l'UE est supérieure à 10 alors l'UE est validée. La compensation entre les UEs d'un même semestre et du même domaine est possible.

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUINON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant	X	Enseignants, Enseignants-chercheurs et professionnels
En contrat d'apprentissage	X	

Après un parcours de formation continue	X	Enseignants, Enseignants-chercheurs et professionnels
En contrat de professionnalisation	X	Enseignants, Enseignants-chercheurs et professionnels
Par candidature individuelle	X	Enseignants, Enseignants-chercheurs et professionnels
Par expérience dispositif VAE prévu en 2002	X	Enseignants, Enseignants-chercheurs et professionnels

	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 :

Arrêté du 25 avril 2002 publié au JO du 27 avril 2002

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

Arrêté du 3 juillet 2015, numéro d'accréditation 20150567

Référence du décret et/ou arrêté VAE :

Décret N°2002-590 du 24 avril 2002

Références autres :

Pour plus d'informations

Statistiques :

www.univ-valenciennes.fr

<http://www.univ-valenciennes.fr>

Autres sources d'information :

www.univ-valenciennes.fr/ISTV

Lieu(x) de certification :

Université de Valenciennes et du Hainaut Cambrésis (UVHC)

Le Mont Houy

59313 Valenciennes cedex 9

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

Institut des Sciences et Technologies de Valenciennes (ISTV)

Université de Valenciennes et du Hainaut Cambrésis (UVHC)

Le Mont Houy

59313 Valenciennes cedex 9

Historique de la certification :