

Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 12568**

Intitulé

MASTER : MASTER Master à finalité Professionnelle et Recherche Domaine : Sciences, technologies, santé Mention : Informatique Spécialité :

Sécurité des systèmes informatiques

Nouvel intitulé : Mention Informatique

AUTORITÉ RESPONSABLE DE LA CERTIFICATION	QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION
Université Paris-Est Créteil Val-De-Marne, Ministère chargé de l'enseignement supérieur	Président de l'université de Paris XII, Recteur de l'académie

Niveau et/ou domaine d'activité

I (Nomenclature de 1967)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

11 Mathématiques et sciences, 326 Informatique, traitement de l'information, réseaux de transmission

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

Ces professionnels peuvent intervenir sur des problèmes posés par la sécurité et les champs d'application qui en découlent que, ils possèdent la capacité à maîtriser les méthodes de modélisation et d'analyse des problèmes de sécurité liés au développement et à l'implémentation des politiques de protection des systèmes informatiques adaptées à différents environnements.

A l'issue du Master à finalité Professionnelle et Recherche, Domaine Sciences, technologies, santé, Mention Informatique, Spécialité Sécurité des systèmes informatiques, le diplômé est capable de :

- Concevoir et mettre en oeuvre des politiques de sécurité dans des environnements variés.
- Analyser la vulnérabilité et les potentialités de sécurisation d'une infrastructure ; détecter ses failles et marges d'amélioration.
- Modéliser les problèmes de sécurité des données, du matériel, des réseaux, des systèmes d'exploitation et des applications.
- Réagir aux attaques, réparer un système endommagé.
- Identifier les origines d'un dommage ; fiabiliser les systèmes de détection, d'intrusion et de sauvegarde.
- Préconiser et fournir des solutions équilibrées tenant compte des contraintes techniques, organisationnelles, relationnelles.
- Convaincre les décideurs et les utilisateurs de l'importance des risques encourus et du bien-fondé des procédures envisagées ou déjà en cours.
- Organiser l'implémentation des décisions politiques, réglementaires, techniques (concernant la sécurité informatique) auprès de tout type d'utilisateur.
- Assurer une veille technologique sur les évolutions en matière de risques et de parades

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

- Automobile,
- Aéronautique
- Construction
- Activités
- Informatiques
- Ingénierie-R&D
- Banque assurances
- Conseil et gestion en entreprises
- Finances
- Informatique industrielle
- Système, réseaux, DATA
- Recherche, études techniques
- Etudes socio économiques
- Expertise assistance technique
- Méthodes, contrôle, qualité
 - Consultant(e) junior sécurité
- Chef de projet e-administration
- Ingénieur(e) réseaux et internet
- Ingénieur(e) méthode qualité et sécurité
- Ingénieur(e) nouvelles technologies de l'information et la communication
- Expert(e) en sécurité des systèmes d'exploitation
- Responsable de la sécurité des systèmes d'information
- Responsable des systèmes informatiques
- Responsable sécurité des systèmes d'information

Codes des fiches ROME les plus proches :

M1802 : Expertise et support en systèmes d'information

M1803 : Direction des systèmes d'information

M1804 : Études et développement de réseaux de télécoms

M1805 : Études et développement informatique

K2108 : Enseignement supérieur

Modalités d'accès à cette certification**Descriptif des composantes de la certification :**

L'étudiant(e) titulaire d'un master 1 des domaines :

Informatique et sciences de l'ingénieur

attestant qu'il ou elle maîtrise les matières fondamentales d'un niveau de master 1 de Informatique,

peut accéder à la deuxième année dès lors qu'il ou elle a satisfait aux conditions d'admission propres à la

commission d'admission de l'UFR de Sciences et technologie.

L'octroi du diplôme s'effectue après une formation en 4 semestres de M1 et de M2 décrits ci-dessous :

Descriptif des composantes de la certification :

Master 1 – semestres 1 et 2 – 60 ECTS

Semestre 1

UE 1 : Calculabilité et complexité (4 ECTS)

UE 2 : Langages de spécification des logiciels (4 ECTS)

UE 3 : Fonctionnement des réseaux (4 ECTS)

UE 4 : Bases de données avancées (4 ECTS)

UE 5 : Anglais scientifique (3 ECTS)

UE 6 : Culture professionnelle (3 ECTS)

UE optionnelles (2 à choisir parmi 4) : Algorithmique avancée (4 ECTS), Nouvelles technologies des réseaux (4 ECTS), Types et programmation (4 ECTS), Logique et programmation (4 ECTS)

Semestre 2

UE Obligatoires : UE 1 : Informatique et société (3 ECTS), UE 2 : Anglais scientifique (3 ECTS), UE 3 : Projet d'informatique (4 ECTS),

UE Optionnelles (5 à choisir parmi 11) : Cryptologie et applications (4 ECTS), Méthodes et outils de vérification (4 ECTS), Initiation à la sécurité (4 ECTS), Sûreté de fonctionnement des systèmes informatiques (4 ECTS), Spécification de la concurrence (4 ECTS), Sémantique des langages de programmation (4 ECTS), Algorithmes distribués et parallèles (4 ECTS), Optimisation (4 ECTS), Statistiques : M1 Mathématiques (4 ECTS), Ondelettes et traitement du signal : M1 Mathématiques (4 ECTS), Processus et finance : M1 Mathématiques (4 ECTS)

Master 2 – semestres 3 et 4 – 60 ECTS

Semestre 3

UE 1 : Fondements de la sécurité : FOSE (3 ECTS)

UE 2 : Méthodes de sécurisation des données : MOSD (3 ECTS)

UE 3 : Sécurité des réseaux : SERE (3 ECTS)

UE 4 : Sécurité des systèmes d'exploitation : SESE (3 ECTS)

UE 5 : Anglais (3 ECTS)

*Parcours recherche ou professionnel : 5 options à choisir parmi MOSC, MEVS, PSSR, MSSI, TYSE, MOSS,

FIAB, MEPO et MEDI :

Modélisation des systèmes communicants: MOSC (3 ECTS), Méthodes de vérification de sécurité : MEVS (3 ECTS), Programmation et sûreté des systèmes répartis : PSSR (3 ECTS), Méthodes de spécification pour des systèmes d'information sécurisés : MSSI (3 ECTS), Types et sécurité : TYSE (3 ECTS), Modélisation de systèmes sécurisés : MOSS (3 ECTS), Méthodes pratiques de développement de politiques de sécurité : MEPO (3 ECTS), Evaluation de la fiabilité et des performances : FIAB (3 ECTS), Méthodes pratiques et outils de détection d'intrusions : MEDI (3 ECTS)

Semestre 4

*Parcours Recherche : Stage de 5 à 6 mois de mars à août (28 ECTS), Initiation recherche (2 ECTS)

**Parcours Professionnel : Stage de 5 à 6 mois de mars à août (24 ECTS), Projet de synthèse professionnel (5 ECTS), Conférences (1 ECTS)

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION QUINON	COMPOSITION DES JURYS	
Après un parcours de formation sous statut d'élève ou d'étudiant	X	Personnes ayant contribué aux enseignements (Loi n°84-52 du 26 janvier 1984 modifiée sur l'enseignement supérieur) 85% enseignants et 15% professionnels
En contrat d'apprentissage	X	

Après un parcours de formation continue	X	Responsable de la formation continue et responsable de la spécialité
En contrat de professionnalisation	X	Personnes ayant contribué aux enseignements (Loi n°84-52 du 26 janvier 1984 modifiée sur l'enseignement supérieur)
Par candidature individuelle	X	Personnes ayant contribué aux enseignements (Loi n°84-52 du 26 janvier 1984 modifiée sur l'enseignement supérieur) 85% enseignants et 15% professionnels
Par expérience dispositif VAE prévu en 2002	X	Cette formation est accessible via : - la Validation des Acquis Professionnels (VAP) qui permet un accès dérogatoire à une formation (décret n°85-9 06 du 23 août 1985) Examen du dossier constitué des cursus de formation, professionnel et personnel par une commission pédagogique. - la Validation des Acquis de l'Expérience (VAE) permettant d'obtenir tout ou partie d'un diplôme (loi de modernisation sociale du 17 janvier 2002, décret n°2002-590 du 24 avril 2002) Examen du dossier constitué des cursus de formation, professionnel et personnel et audition du candidat par un jury de validation. Tous les diplômes proposés à l'université Paris-Est Créteil Val de Marne sont susceptibles de faire l'objet d'une VAP ou d'une VAE.

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

LIENS AVEC D'AUTRES CERTIFICATIONS	ACCORDS EUROPÉENS OU INTERNATIONAUX
	Accords universitaires partenaires : - ENSIIE Laboratoires de recherche partenaires : - IBISC FRE CNRS 2873 Vérification, réseaux, algorithmique - LACL EA 4219 Sécurité, sûreté, vérification, logique - SAMOVAR UMR 5157 INT-CNRS Sécurité, Réseaux, Génie logiciel

Base légale

Référence du décret général :

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

Arrêté du 25 avril 2002 relatif au diplôme national de master publié au JO du 27 avril 2002

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

<http://www.u-pec.fr/pratiques/universite/observatoire-etudiant/enquetes-d-insertion-professionnelle-336228.kjsp?rh=1181035608921>

Autres sources d'information :

<http://lacl.univ-paris12.fr/LMD/master.html>

<http://sciences-tech.u-pec.fr/>

Statistiques

Master Mention Informatique Sécurité des Systèmes Informatiques

Faculté des sciences et technologie

Université Paris-Est Créteil Val de Marne

Lieu(x) de certification :

Université Paris-Est Créteil Val de Marne
61, avenue du Général de Gaulle
94010 Créteil Cedex

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

Créteil - CMC
Université Paris-Est Créteil Val de Marne
Faculté des sciences et technologie
61, avenue du Général de Gaulle
94010 Créteil Cedex

Historique de la certification :

Le master existe depuis 2005 et comportait deux spécialités en co-habilitation avec l'Université d'Evry, l'ENSIIE et Télécom-Sud Paris: MOPS (localisée à Evry) et SSI (localisée à Paris 12). Depuis 2009, seule l'université Paris-Est, Créteil propose le master d'informatique, spécialité SSI.

Certification suivante : Mention Informatique