CERTIFICATION PROFESSIONNELLE

BUT - Réseaux & Télécommunications : Cybersécurité

Code de la fiche : **RNCP35455**

Etat : **Active**

Télécharger la fiche | Aide en ligne | Supplément Europass : FR - EN

L'essentiel

Certification remplacée par	**RNCP41611 -** BUT - Réseaux & télécommunications : Cybersécurité
Nomenclature du niveau de qualification	**Niveau 6**
Code(s) NSF	**326p :** Informatique, traitement de l'information (organisation, gestion) **326n :** Analyse informatique, conception d'architecture de réseaux **326 :** Informatique, traitement de l'information, réseaux de transmission
Formacode(s)	**31045 :** Cybersécurité
Date de début des parcours certifiants	**01-09-2021**
Date d'échéance de l'enregistrement	**31-08-2026**

Certificateur(s) Résumé de la certification Blocs de compétences Secteur d'activité et type d'emploi Voie d'accès

Liens avec d'autres certifications professionnelles, certifications ou habilitations Base légale Pour plus d'informations

Certificateur(s)

Nom légal	Siret	Nom commercial	Site internet
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE	11004401300040	-	-
LA ROCHELLE UNIVERSITE - UNIVERSITE DE LA ROCHELLE	19170032700015	-	-
NANTES UNIVERSITE	13002974700016	-	-
UNIVERSITE BOURGOGNE EUROPE	93823061200013	-	-
UNIVERSITE CLERMONT AUVERGNE	13002806100013	-	-
UNIVERSITE COTE D'AZUR	13002566100013	-	-
UNIVERSITE D ARTOIS	19624401600016	-	-
UNIVERSITE D'AIX MARSEILLE	13001533200013	-	-
UNIVERSITE DE CAEN NORMANDIE	19141408500016	-	-
UNIVERSITE DE HAUTE ALSACE	19681166500013	-	-
UNIVERSITE DE LA GUYANE	13002059700014	-	-
UNIVERSITE DE LA REUNION	19974478000016	-	-
UNIVERSITE DE LORRAINE	13001550600012	-	-
UNIVERSITE DE MONTPELLIER	13002979600013	-	-
UNIVERSITE DE PAU ET DES PAYS DE L'ADOUR (UPPA)	19640251500270	-	-
UNIVERSITE DE REIMS CHAMPAGNE-ARDENNE (URCA)	19511296600799	-	-
UNIVERSITE DE RENNES	13003051300019	-	-
UNIVERSITE DE TOURS	19370800500478	-	-

Nom légal	Siret	Nom commercial	Site internet
UNIVERSITE GRENOBLE ALPES	13002608100013	-	-
UNIVERSITE JEAN MONNET (EPSCP)	93850168100010	-	-
UNIVERSITE MARIE ET LOUIS PASTEUR (UMLP)	93810656400017	-	-
UNIVERSITE PARIS EST CRETEIL VAL DE MARNE	19941111700013	-	-
UNIVERSITE PARIS XIII PARIS NORD VILLETANEUSE	19931238000017	-	-
UNIVERSITE SAVOIE MONT BLANC	19730858800015	-	-
UNIVERSITE TOULOUSE II	19311383400017	-	-
UNIVERSITE VERSAILLES ST QUENTIN YVELINE	19781944400013	-	-

Résumé de la certification

Objectifs et contexte de la certification :

Les diplômés du BUT - Réseaux & Télécommunications - Cybersécurité auront l'ensemble des bases théoriques, techniques et méthodologiques pour analyser les risques d'attaques menaçant le Système d'Information (SI) d'une entreprise (réseaux, serveurs, postes de travail, ...). Ils sont en mesure de définir la politique de sécurité du SI de l'entreprise (PSSI) visant à fixer le cadre d'utilisation des ressources numériques, à sensibiliser et former les utilisateurs.

Les certifiés connaissent et applique au sein de l'entreprise la loi (RGPD, ...) et les préconisations de l'état (ANSSI) imposées par le contexte actuel. Ils conçoivent et déploient une architecture de réseaux et systèmes répondant aux contraintes de sécurité informatique et légales définies précédemment. Pour y parvenir, ils administrent la sécurité du matériel (serveurs, routeurs, commutateurs, firewall, sondes, contrôleurs, ...), des systèmes d'exploitation (hyperviseurs, Linux, Windows, ...), des services et logiciels (Web, messagerie, DNS, VPN, authentification, cryptologie, anti-virus, anti-malware, IDS/IPS, ...). Ils utilisent des outils de tests de pénétration suivant une méthodologie permettant de garantir la robustesse du Système d'Information. Afin qu'il reste fiable et opérationnel, ils assurent sa surveillance permanente et peuvent ainsi garantir et faire évoluer sa sécurité.

Grâce aux outils de supervision, ils sont capables d'identifier des attaques, d'alerter les utilisateurs, la hiérarchie et d'appliquer des solutions de remédiations. Si toutefois un incident devait intervenir, ce qui doit toujours rester une éventualité, ils participeront à la gestion de crise. Ils sauront isoler le SI, constituer les preuves de l'attaque (sauvegarde des fichiers infectés, logs, images de la mémoire et disques, ...) et appliquer les plans de reprise d'activité (PRA/PCA). Enfin, ils pourront participer aux analyses post-incidents des preuves récoltées.

Activités visées :

Administration des réseaux et de l'Internet o Conception et administration de l'infrastructure du réseau informatique d'une entreprise o Installation et administration des services réseau informatique d'une entreprise o Déploiement et administration des solutions fixes pour les clients d'un opérateur de télécommunication ·

Connexion des entreprises et des usages o Déploiement des supports et systèmes de transmission o Mise en service et administration des équipements d'accès fixe ou mobile d'un opérateur de télécommunications o Déploiement et administration des accès sans fil pour l'entreprise o Déploiement des systèmes de communications ·

Création d'outils et d'applications informatiques pour les R&T o Conception, déploiement et maintenance du système d'information d'une entreprise o Automatisation du déploiement et de la maintenance des outils logiciels o Développement d'outils informatiques à usage interne d'une équipe. ·

Administration d'un système d'information sécurisé o Analyse de l'existant et étude des besoins de sécurité d'une petite structure o Évolution et mise en conformité du système d'information d'une entreprise ·

Surveillance d'un système d'information sécurisé o Surveillance et analyse du système d'information o Audit de sécurité o Gestion d'un incident de sécurité.

Compétences attestées :

Administrer les réseaux et l'Internet o En choisissant les solutions et technologies réseaux adaptées o En respectant les principes fondamentaux de la sécurité informatique o En utilisant une approche rigoureuse pour la résolution des dysfonctionnements o En respectant les règles métiers o En assurant une veille technologique. ·

Connecter les entreprises et les usagers o En communiquant avec le client et les différents acteurs impliqués, parfois en anglais o En faisant preuve d'une démarche scientifique o En choisissant les solutions et technologies adaptées o En proposant des solutions respectueuses de l'environnement. ·

Créer des outils et applications informatiques pour les R&T o En étant à l'écoute des besoins du client o En documentant le travail réalisé o En utilisant les outils numériques à bon escient o En choisissant les outils de développement adaptés o En intégrant les problématiques de sécurité ·

Administrer un système d'information sécurisé o En visant un juste compromis entre exigences de sécurité et contraintes d'utilisation o En respectant les normes et le cadre juridique o En intégrant les dernières technologies o En travaillant en équipe o En sensibilisant efficacement des utilisateurs. ·

Surveiller un système d'information sécurisé o En assurant une veille permanente o En réalisant les mises à jour critiques o En automatisant des tâches o En s'intégrant dans une équipe o En surveillant le comportement du réseau o En veillant au respect des contrats et à la conformité des obligations du système d'information.

Compétences transverses:

Se servir du numériques : En utilisant les outils numériques de référence et les règles de sécurité informatique pour acquérir, traiter, produire et diffuser de l'information ainsi que pour collaborer en interne et en externe.

Exploiter des données à des fins d'analyse : En Identifiant, sélectionnant et analysant avec esprit critique diverses ressources dans son domaine de spécialité pour documenter un sujet et synthétiser ces données en vue de leur exploitation. · En analysant et synthétisant des données en vue de leur exploitation. · En développant une argumentation avec esprit critique.

S'exprimer et communiquer à l'écrit et à l'oral : En se servant aisément des différents registres d'expression écrite et orale de la langue française. Communiquer par oral et par écrit, de façon claire et non-ambiguë, dans au moins une langue étrangère.

Se positionner vis à vis d'un champ professionnel : · En identifiant et en situant les champs professionnels potentiellement en relation avec les acquis et la mention ainsi que les parcours possibles pour y accéder · En Caractérisant et en valorisant son identité, ses compétences et son projet professionnel en fonction d'un contexte · En identifiant le processus de production, de diffusion et de valorisation des savoirs

Agir en responsabilité au sein d'une organisation professionnelle : · En Situant son rôle et sa mission au sein d'une organisation pour s'adapter et prendre des initiatives · En respectant les principes d'éthique, de déontologie et de responsabilité environnementale · En travaillant en équipe et en réseau ainsi qu'en autonomie et responsabilité au service d'un projet · En analysant ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique · En prenant en compte des problématiques liées aux situations de handicap, à l'accessibilité et à la conception universelle.

Modalités d'évaluation :

Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet).

Blocs de compétences

RNCP35455BC01 - Administrer les réseaux et l'Internet

Liste de compétences	Modalités d'évaluation
- Maîtriser les lois fondamentales de l'électricité afin d'intervenir sur des équipements de réseaux et télécommunications - Comprendre l'architecture des systèmes numériques et les principes du codage de l'information - Configurer les fonctions de base du réseau local - Maîtriser les rôles et les principes fondamentaux des systèmes d'exploitation afin d'interagir avec ceux-ci pour la configuration et administration des réseaux et services fournis - Identifier les dysfonctionnements du réseau local - Installer un poste client. - Configurer et dépanner le routage dynamique dans un réseau - Configurer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau - Déployer des postes clients et des solutions virtualisées - Déployer des services réseaux avancés et systèmes de supervision - Identifier les réseaux opérateurs et l'architecture d'Internet - Travailler en équipe - Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS et de sécurité - Réaliser la documentation technique de ce projet - Réaliser une maquette de démonstration du projet - Défendre/argumenter un projet - Communiquer avec les acteurs du projet - Gérer le projet et les différentes étapes de sa mise en oeuvre en respectant les délais	Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet)

RNCP35455BC02 - Connecter les entreprises et les usagers

Liste de compétences	Modalités d'évaluation
- Mesurer et analyser les signaux - Caractériser des systèmes de transmissions élémentaires et découvrir la modélisation mathématique de leur fonctionnement - Déployer des supports de transmission - Connecter les systèmes de ToIP - Communiquer avec un client ou	Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet)

Liste de compétences	Modalités d'évaluation
un collaborateur - Déployer et caractériser des systèmes de transmissions complexes - Mettre en place un accès distant sécurisé - Mettre en place une connexion multi-site via un réseau opérateur - Administrer les réseaux d'accès des opérateurs - Organiser un projet pour répondre au cahier des charges - Déployer un système de communication pour l'entreprise - Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité - Déployer un réseau d'accès fixes ou mobile pour un opérateur de télécommunications en intégrant la sécurité - Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise - Collaborer en mode projet en français et en anglais	

RNCP35455BC03 - Créer des outils et applications informatiques pour les R&T

Liste de compétences	Modalités d'évaluation
- Utiliser un système informatique et ses outils - Lire, exécuter, corriger et modifier un programme - Traduire un algorithme, dans un langage et pour un environnement donné - Connaître l'architecture et les technologies d'un site Web - Choisir les mécanismes de gestion de données adaptés au développement de l'outil - S'intégrer dans un environnement propice au développement et au travail collaboratif - Automatiser l'administration système avec des scripts - Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles - Utiliser un protocole réseau pour programmer une application client/serveur - Installer, administrer un système de gestion de données	Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet)

Liste de compétences	Modalités d'évaluation
- Accéder à un ensemble de données depuis une application et/ou un site web - Élaborer les spécifications techniques et le cahier des charges d'une application informatique - Mettre en place un environnement de travail collaboratif - Participer à la formation des utilisateurs - Déployer et maintenir une solution informatique - S'informer sur les évolutions et les nouveautés technologiques - Sécuriser l'environnement numérique d'une application	

RNCP35455BC04 - Administrer un système d'information sécurisé

Liste de compétences	Modalités d'évaluation
- Utiliser les bonnes pratiques et les recommandations de cybersécurité - Mettre en oeuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau - Sécuriser les systèmes d'exploitation - Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information - Connaître les différents types d'attaque - Comprendre des documents techniques en anglais - Participer activement à une analyse de risque pour définir une politique de sécurité pour une petite structure - Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau - Sécuriser les services - Proposer une architecture sécurisée de système d'information pour une petite structure	Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet)

RNCP35455BC05 - Surveiller un système d'information sécurisé

Liste de compétences	Modalités d'évaluation

Liste de compétences	Modalités d'évaluation
- Administrer les outils de surveillance du système d'information - Administrer les protections contre les logiciels malveillants - Automatiser les tâches d'administration - Prendre en main des outils de test de pénétration réseau/ système - Surveiller l'activité du système d'information - Appliquer une méthodologie de tests de pénétration - Gérer une crise suite à un incident de sécurité	Validation des compétences par évaluation orale, écrite et pratique lors de mises en situation professionnelle (rédaction et réalisation de rapports, plans, schémas, études techniques - exposé oral de présentation d'équipement ou de procédé - mise en situation sur des pilotes et en stage et projet, études de cas, évaluation du travail réalisé en stage et projet)

RNCP35455BC06 - Usages numériques

Liste de compétences	Modalités d'évaluation
Utiliser les outils numériques de référence et les règles de sécurité informatique pour acquérir, traiter, produire et diffuser de l'information ainsi que pour collaborer en interne et en externe.	*Contrôle continu intégral mobilisant notamment des mises en situation professionnelle à partir desquelles est demandée une démarche autoréflexive et de démonstration des compétences acquises*

RNCP35455BC07 - Exploitation de données à des fins d'analyse

Liste de compétences	Modalités d'évaluation
Identifier, sélectionner et analyser avec esprit critique diverses ressources dans son domaine de spécialité pour documenter un sujet et synthétiser ces données en vue de leur exploitation. · Analyser et synthétiser des données en vue de leur exploitation. · Développer une argumentation avec esprit critique.	*Contrôle continu intégral mobilisant notamment des mises en situation professionnelle à partir desquelles est demandée une démarche autoréflexive et de démonstration des compétences acquises*

RNCP35455BC08 - Expression et communication écrites et orales

Liste de compétences	Modalités d'évaluation
Se servir aisément des différents registres d'expression écrite et orale de la langue française. Communiquer par oral et par écrit, de façon claire et non-ambiguë, dans au moins une langue étrangère.	*Contrôle continu intégral mobilisant notamment des mises en situation professionnelle à partir desquelles est demandée une démarche autoréflexive et de démonstration des compétences acquises*

RNCP35455BC09 - Action en responsabilité au sein d'une organisation professionnelle

Liste de compétences	Modalités d'évaluation
Situer son rôle et sa mission au sein d'une organisation pour s'adapter et prendre des initiatives · Respecter les principes d'éthique, de déontologie et de responsabilité environnementale · Travailler en équipe et en réseau ainsi qu'en autonomie et responsabilité au service d'un projet · Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique · Prendre en compte des problématiques liées aux situations de handicap, à l'accessibilité et à la conception universelle.	*Contrôle continu intégral mobilisant notamment des mises en situation professionnelle à partir desquelles est demandée une démarche autoréflexive et de démonstration des compétences acquises*

RNCP35455BC10 - Positionnement vis à vis d'un champ professionnel

Liste de compétences	Modalités d'évaluation
Identifier et situer les champs professionnels potentiellement en relation avec les acquis et la mention ainsi que les parcours possibles pour y accéder · Caractériser et valoriser son identité, ses compétences et son projet professionnel en fonction d'un contexte Identifier le processus de production, de diffusion et de valorisation des savoirs	*Contrôle continu intégral mobilisant notamment des mises en situation professionnelle à partir desquelles est demandée une démarche autoréflexive et de démonstration des compétences acquises*

Description des modalités d'acquisition de la certification par capitalisation des blocs de compétences et/ou par correspondance :

L'intégralité de la certification s'obtient par la validation de tous les blocs de compétences.

Secteur d'activité et type d'emploi

Secteurs d'activités :

Le titulaire d'un BUT **« Réseaux & Télécommunications » : « Cybersécurité »** exerce son activité toutes les entreprises, les organismes privés ou publics qui ont un service informatique.

Type d'emplois accessibles :

Débutant : Technicien des réseaux d'entreprises / en cybersécurité / réseaux sécurisés / d'infrastructures sécurisées, coordinateur cybersécurité des systèmes d'information, administrateur de solutions de sécurité, auditeur de sécurité technique, opérateur analyste SOC, intégrateur de solutions de sécurité, administrateur Data Center

Après 2 ou 3 ans d'expérience : (avec parfois des formations internes entreprise sur des domaines spécialisés et techniques ; Dev, IoT, Cloud, …) Responsable de la sécurité informatique au sein d'une petite structure (IT security manager), Analyste sécurité (Analyst security), Responsable de projet de sécurité (Security project leader), Spécialiste sécurité d'un domaine technique (Technical security expert), Spécialiste en développement sécurisé (Application security expert)

Code(s) ROME :

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

M1804 - Études et développement de réseaux de télécoms

M1810 - Production et exploitation de systèmes d''information

M1801 - Administration de systèmes d''information

M1802 - Expertise et support en systèmes d''information

Références juridiques des règlementations d'activité :

Voie d'accès

Le cas échant, prérequis à l'entrée en formation :

Le cas échant, prérequis à la validation de la certification :

Pré-requis disctincts pour les blocs de compétences :

Non

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
Après un parcours de formation sous statut d'élève ou d'étudiant	X		Jury présidé par le directeur de l'IUT et comprenant les chefs de départements, pour au moins la moitié des enseignants-chercheurs et enseignants, et pour au moins un quart et au plus la moitié de professionnels en relation étroite avec la spécialité concernée, choisies dans les conditions prévues à l'article 612-1 du code de l'éducation.	-
En contrat d'apprentissage	X		Jury présidé par le directeur de l'IUT et comprenant les chefs de départements, pour au moins la moitié des enseignants-chercheurs et enseignants, et pour au moins un quart et au plus la moitié de professionnels en relation étroite avec la spécialité concernée, choisies dans les conditions prévues à l'article 612-1 du code de l'éducation.	-
Après un parcours de formation continue	X		Jury présidé par le directeur de l'IUT et comprenant les chefs de départements, pour au moins la moitié des enseignants-chercheurs et enseignants, et pour au moins un quart et au plus la moitié de professionnels en relation étroite avec la spécialité concernée, choisies dans les conditions prévues à l'article 612-1 du code de l'éducation.	-
En contrat de professionnalisation	X		Jury présidé par le directeur de l'IUT et comprenant les chefs de départements, pour au moins la moitié des enseignants-chercheurs et enseignants, et pour au moins un quart et au plus la moitié de professionnels en relation étroite avec la spécialité concernée, choisies dans les conditions prévues à l'article 612-1 du code de l'éducation.	-
Par candidature individuelle		X	-	-
Par expérience	X		Jury présidé par le directeur de l'IUT et comprenant les chefs de départements, pour au moins la moitié des enseignants-chercheurs et enseignants, et pour au moins un quart et au plus la moitié de professionnels en relation étroite avec la spécialité concernée, choisies dans les conditions prévues à l'article L. 613-4 du code de l'éducation.	-

Oui	Non

	Oui	Non
Inscrite au cadre de la Nouvelle Calédonie	X	
Inscrite au cadre de la Polynésie française	X	

Liens avec d'autres certifications professionnelles, certifications ou habilitations

Lien avec d'autres certifications professionnelles, certifications ou habilitations :

Oui

Certifications professionnelles, certifications ou habilitations en correspondance au niveau européen ou international :

Certifications professionnelles enregistrées au RNCP en correspondance :

Code de la fiche	Intitulé de la certification professionnelle reconnue en correspondance	Nature de la correspondance (totale, partielle)
RNCP29964	**LP Administration et Sécurité des Réseaux**	Partielle
RNCP29968	**LP Licence professionnelle Réseaux Informatiques Mobilité Sécurité**	Partielle
RNCP20649	DUT Réseaux & Télécommunications	Partielle

Liens avec des certifications et habilitations enregistrées au Répertoire spécifique :

Base légale

Référence des arrêtés et décisions publiés au Journal Officiel ou au Bulletin Officiel (enregistrement au RNCP, création diplôme, accréditation...) :

Date du JO/BO	Référence au JO/BO
12/12/2019	Arrêté du 6 décembre 2019 portant réforme de la licence professionnelle

Date de publication de la fiche	16-03-2021
Date de début des parcours certifiants	01-09-2021

Date d'échéance de l'enregistrement	31-08-2026

Pour plus d'informations

Statistiques :

Liste des organismes préparant à la certification :

Liste des organismes préparant à la certification

Historique des changements de certificateurs :

Nom légal du certificateur	Siret du certificateur	Action	Date de la modification
UNIVERSITE CLERMONT AUVERGNE	13002806100013	Est ajouté	16-03-2021
UNIVERSITE COTE D'AZUR	13002566100013	Est ajouté	16-03-2021
UNIVERSITE DE BESANCON - UNIVERSITE DE FRANCHE-COMTE	19251215000363	Est ajouté	16-03-2021
UNIVERSITE DE LORRAINE	13001550600012	Est ajouté	16-03-2021
UNIVERSITE DE MONTPELLIER	13002054800017	Est ajouté	16-03-2021
UNIVERSITE DE NANTES	19440984300019	Est ajouté	16-03-2021
UNIVERSITE DE PAU ET DES PAYS DE L'ADOUR (UPPA)	19640251500270	Est ajouté	16-03-2021
UNIVERSITE DE TOURS	19370800500478	Est ajouté	16-03-2021
UNIVERSITE D'AIX MARSEILLE	13001533200013	Est ajouté	16-03-2021
UNIVERSITE DE CAEN NORMANDIE	19141408500016	Est ajouté	16-03-2021

Nom légal du certificateur	Siret du certificateur	Action	Date de la modification
UNIVERSITE DE HAUTE ALSACE	19681166500013	Est ajouté	16-03-2021
UNIVERSITE DE REIMS CHAMPAGNE-ARDENNE	19511296600435	Est ajouté	16-03-2021
UNIVERSITE DIJON BOURGOGNE	19211237300019	Est ajouté	16-03-2021
UNIVERSITE JEAN MONNET SAINT ETIENNE - TELECOM SAINT ETIENNE	19421095100456	Est ajouté	16-03-2021
UNIVERSITE VERSAILLES ST QUENTIN YVELINE	19781944400013	Est ajouté	16-03-2021
UNIVERSITE TOULOUSE II	19311383400017	Est ajouté	16-03-2021
UNIVERSITE PARIS EST CRETEIL VAL DE MARNE	19941111700013	Est ajouté	16-03-2021
LA ROCHELLE UNIVERSITE - UNIVERSITE DE LA ROCHELLE	19170032700015	Est ajouté	16-03-2021
UNIVERSITE D ARTOIS	19624401600016	Est ajouté	16-03-2021
UNIVERSITE DE LA REUNION	19974478000016	Est ajouté	16-03-2021
UNIVERSITE SAVOIE MONT BLANC	19730858800015	Est ajouté	16-03-2021
UNIVERSITE DE RENNES I	19350936100013	Est ajouté	16-03-2021
UNIVERSITE GRENOBLE ALPES	13002608100013	Est ajouté	16-03-2021
UNIVERSITE PARIS XIII PARIS NORD VILLETANEUSE	19931238000017	Est ajouté	16-03-2021
UNIVERSITE DE NANTES	19440984300019	Est retiré	01-03-2023

Nom légal du certificateur	Siret du certificateur	Action	Date de la modification
UNIVERSITE DE MONTPELLIER	13002054800017	Est retiré	01-03-2023
UNIVERSITE DE RENNES I	19350936100013	Est retiré	01-03-2023
UNIVERSITE DE REIMS CHAMPAGNE-ARDENNE	19511296600435	Est retiré	01-03-2023
UNIVERSITE DE REIMS CHAMPAGNE-ARDENNE (URCA)	19511296600799	Est ajouté	01-03-2023
NANTES UNIVERSITE	13002974700016	Est ajouté	01-03-2023
UNIVERSITE DE MONTPELLIER	13002979600013	Est ajouté	01-03-2023
UNIVERSITE DE RENNES	13003051300019	Est ajouté	01-03-2023
UNIVERSITE DE LA GUYANE	13002059700014	Est ajouté	01-07-2023
UNIVERSITE JEAN MONNET SAINT ETIENNE - TELECOM SAINT ETIENNE	19421095100456	Est retiré	23-09-2024
UNIVERSITE JEAN MONNET SAINT ETIENNE	19421095100423	Est ajouté	23-09-2024
UNIVERSITE DE BESANCON - UNIVERSITE DE FRANCHE-COMTE	19251215000363	Est retiré	05-02-2025
UNIVERSITE MARIE ET LOUIS PASTEUR (UMLP)	93810656400017	Est ajouté	05-02-2025
UNIVERSITE JEAN MONNET SAINT ETIENNE	19421095100423	Est retiré	03-03-2025
UNIVERSITE JEAN MONNET (EPSCP)	93850168100010	Est ajouté	03-03-2025
UNIVERSITE DIJON BOURGOGNE	19211237300019	Est retiré	03-03-2025
UNIVERSITE BOURGOGNE EUROPE	93823061200013	Est ajouté	03-03-2025

Nouvelle(s) Certification(s) :

Code de la fiche	Intitulé de la certification remplacée
RNCP41611	BUT - Réseaux & télécommunications : Cybersécurité

Référentiel d'activité, de compétences et d'évaluation :

Référentiel d'activité, de compétences et d'évaluation