

Pourquoi cette UE ?

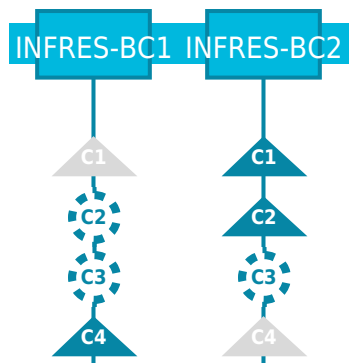
Ce module permet à l'élève de maîtriser les bases de la cryptographie et la gestion des certificats, essentielles à la sécurisation des communications et des infrastructures. Il met un accent particulier sur la mise en œuvre de ces mécanismes dans un environnement cloud privé basé sur OpenStack. L'élève apprend à déployer, configurer et sécuriser une plateforme OpenStack, compétence stratégique pour la gestion d'infrastructures virtualisées, souveraines et évolutives, en réponse aux besoins actuels des organisations.

Éléments constitutifs de l'UE

		coefficient
INFRES_7_2_SR-1 Cryptographie et preuve numérique		2
INFRES_7_2_SR-2 Applications de la cryptographie		1
INFRES_7_2_SR-3 Infrastructure: open stack		2
INFRES_7_2_SR-4 A supprimer !!!		1
Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
72	14	4

Alignement curriculaire

Parmi les compétences visées par la formation, lesquelles sont développées dans cette UE ?



BC1	L'UE ne contribue pas à ce bloc de compétences
BC1	L'UE contribue à ce bloc de compétences
C1	Compétence non adressée dans cette UE
C1	Compétence mise en œuvre dans cette UE
C1	Compétence enseignée dans cette UE
C1	Compétence évaluée dans cette UE
C1	Compétence enseignée et évaluée dans cette UE

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-1 Cryptographie et preuve numérique	S7

Contexte et enjeux de l'enseignement

Dans un monde de plus en plus interconnecté, la protection des données, la confidentialité des échanges et l’intégrité des systèmes numériques sont devenues des enjeux cruciaux. La cryptographie constitue le socle technique garantissant ces propriétés, tant dans les communications que dans le stockage et les traitements décentralisés. L’élève ingénieur doit comprendre comment concevoir, analyser et mettre en œuvre des primitives cryptographiques sûres, mais aussi comment prouver mathématiquement leur sécurité. Cet enseignement prépare à appréhender des systèmes critiques tels que les paiements électroniques, les réseaux sécurisés, les blockchains et les identités numériques. Une attention particulière est portée à la rigueur des preuves, à la résistance aux attaques et à l’implémentation sûre dans des environnements contraints.

Prise en compte des dimensions socio-environnementales

Prérequis
Aucun

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	14
Cours intégré (cours + TD)	
TD	
TP	10
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	4

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Expliquer les principes fondamentaux de la cryptographie moderne.
- Concevoir des protocoles cryptographiques simples et sûrs.
- Analyser la sécurité d’un système à l’aide de preuves formelles.
- Identifier les vulnérabilités cryptographiques courantes.
- Implémenter des primitives de manière correcte et résistante aux attaques.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP de mise en place de certificats

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

QCM

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-1 Cryptographie et preuve numérique	S7

Plan de cours

- Fondements mathématiques : rappels sur les structures algébriques (groupes, anneaux, corps), complexité calculatoire, fonctions à sens unique, et hypothèses de sécurité.
- Primitives cryptographiques : chiffrement symétrique (AES, modes opératoires), chiffrement asymétrique (RSA, Diffie-Hellman, courbes elliptiques), fonctions de hachage, MAC, signatures numériques.
- Modèles et preuves de sécurité : définition de la sécurité (IND-CPA, IND-CCA, EUF-CMA...), modèles d'attaques, cadres formels pour prouver la robustesse des constructions cryptographiques.
- Protocoles cryptographiques : protocoles d'authentification, échanges de clés, canaux chiffrés, signatures aveugles, preuves à divulgation nulle de connaissance.
- Implémentation sécurisée et cas d'usage : bonnes pratiques de développement, contre-mesures aux attaques par canaux auxiliaires, étude de cas (TLS, chiffrement disque, messageries sécurisées, blockchain, etc.).

Ressources et références

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 297

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-2 Applications de la cryptographie	S7

Objectifs pédagogiques	Activités	Évaluations et retours faits aux élèves
(à la fin de cet enseignement, l'étudiant sera capable de ...) - Expliquer le rôle et les principes des certificats numériques. - Déployer une autorité de certification et ses composants associés. - Gérer le cycle de vie complet des certificats dans un SI. - Automatiser l'émission et le renouvellement de certificats. - Identifier et résoudre les incidents liés aux certificats.	(CM, TD, TP, projet, sortie terrain, etc.) Cours TP de déploiement et gestion de certificat sur un environnement Windows	(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...) QCM TP évalué

Plan de cours

- Écosystème PKI et architecture d'une autorité de certification
- Modèles hiérarchiques et distribués
- Fonctionnement d'une CA racine et intermédiaire
- Infrastructure matérielle et logicielle associée
- Cycle de vie d'un certificat
- Génération de clés, demandes de certificats (CSR)
- Délivrance, publication, renouvellement et révocation
- Listes de révocation (CRL), OCSP, durée de vie et rotation
- Automatisation et intégration dans les systèmes d'information
- Protocoles ACME, SCEP, EST
- Intégration avec les serveurs web, systèmes internes, IoT
- Sécurité des processus automatisés
- Surveillance, gestion des incidents et conformité
- Détection des pannes liées aux certificats
- Bonnes pratiques de surveillance et d'alerte
- Audits, conformité réglementaire (eIDAS, RGPD, etc.)

Ressources et références

Cryptographie

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-3 Infrastructure: open stack	S7

Contexte et enjeux de l'enseignement

Le développement rapide des services numériques exige des infrastructures cloud flexibles, scalables et maîtrisées. OpenStack, solution open source de cloud computing, permet de déployer des environnements IaaS (Infrastructure as a Service) comparables à ceux des grands fournisseurs commerciaux, tout en gardant le contrôle sur les données et l'architecture. Son adoption croissante dans les secteurs publics, industriels et scientifiques répond à un besoin d'autonomie technologique, d'optimisation des ressources matérielles, et de standardisation des déploiements. Cet enseignement prépare les élèves ingénieurs à concevoir, administrer et sécuriser des infrastructures cloud complexes basées sur OpenStack, en lien avec les enjeux actuels de souveraineté numérique, d'automatisation des systèmes et d'intégration DevOps.

Prise en compte des dimensions socio-environnementales

Prérequis
Administration Linux Virtualisation

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	9
Cours intégré (cours + TD)	
TD	
TP	15
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	9

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Expliquer l'architecture et les composants d'OpenStack.
- Déployer une infrastructure OpenStack sur un cluster.
- Gérer les services IaaS (réseaux, instances, volumes).
- Intégrer OpenStack dans un environnement DevOps.
- Diagnostiquer et sécuriser une infrastructure cloud OpenStack.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP de mise en place d'une architecture Open Stack sur machine virtuelle

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

QCM
TP évalué

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-3 Infrastructure: open stack	S7

Plan de cours

Introduction au cloud computing et à OpenStack Présentation des paradigmes IaaS, PaaS, SaaS. Architecture modulaire d'OpenStack. Cas d'usage industriels et publics. Comparaison avec les offres cloud propriétaires. - Installation et configuration de base d'OpenStack - Prise en main des outils de déploiement (DevStack, Packstack, kolla-ansible). Configuration réseau, stockage et compute. Mise en place d'un environnement de test sur machines virtuelles ou cluster réel. - Administration des services OpenStack Gestion des projets, utilisateurs et droits. Création et gestion d'instances virtuelles. Configuration des réseaux virtuels (Neutron), des volumes (Cinder), et des images (Glance). Monitoring et journalisation. - Sécurité, haute disponibilité et performances Principes de sécurité dans OpenStack. Isolation des tenants, gestion des accès. Approches de redondance, tolérance aux pannes et mise à l'échelle. Optimisation des ressources. - Automatisation, intégration et supervision Automatisation des déploiements avec Ansible. Intégration CI/CD dans un environnement OpenStack. Supervision avancée avec Prometheus, Grafana, ou Stacklight. Perspectives d'évolution du cloud souverain.	
--	--

Ressources et références

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 297

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-4 A supprimer !!!	S7

Contexte et enjeux de l'enseignement

Prise en compte des dimensions socio-environnementales

Prérequis

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	6
Cours intégré (cours + TD)	
TD	
TP	6
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 258

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 261

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 264

INFRES_7_2_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_SR-4 A supprimer !!!	S7

Plan de cours

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 292

Ressources et références

Deprecated: htmlspecialchars(): Passing null to parameter #1 (\$string) of type string is deprecated in C:\Developpement\syllabus\public_html\views\syllabus_template.php on line 297