

Pourquoi cette UE ?

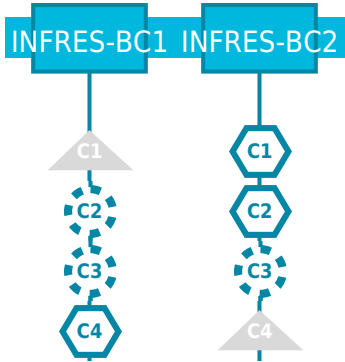
Ce module forme les élèves aux fondements de la sécurité des systèmes informatiques, en lien direct avec les pratiques DevOps. La cryptographie leur permet de comprendre les mécanismes de confidentialité et d'intégrité. La gestion des certificats leur donne les compétences pour sécuriser les communications et les accès. L'infrastructure as code complète l'approche en automatisant le déploiement d'environnements sécurisés, traçables et reproductibles. Ce module renforce l'autonomie et la rigueur des élèves face aux exigences de la production.

Éléments constitutifs de l'UE

		coefficient
INFRES_7_2_DL-1 Cryptographie et preuve numérique		2
INFRES_7_2_DL-2 Application de la cryptographie		1
INFRES_7_2_DL-3 Infrastructure as code		1
Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
48	5	3

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_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-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_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-2 Application de la cryptographie	S7

Contexte et enjeux de l'enseignement

Dans un environnement numérique où la sécurité des communications, l'identité des équipements et la confiance dans les échanges sont essentielles, la gestion du cycle de vie des certificats constitue un pilier fondamental. De la génération à la révocation, en passant par le déploiement et le renouvellement, chaque étape doit être maîtrisée pour garantir la continuité des services et la sécurité des infrastructures. Cet enseignement prépare les élèves à concevoir et maintenir des systèmes de gestion de certificats robustes, adaptés aux exigences industrielles, réglementaires et techniques. Il aborde également les défis liés à l'automatisation, à l'intégration dans les systèmes distribués et aux politiques de sécurité.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	7
Cours intégré (cours + TD)	
TD	
TP	4
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	1

Objectifs pédagogiques

(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.

Activités

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

Cours
TP de déploiement et gestion de certificat sur un environnement Windows

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_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-2 Application de la cryptographie	S7

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_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-3 Infrastructure as code	S7

Contexte et enjeux de l'enseignement

L’infrastructure as code (IaC) transforme la gestion des systèmes d’information en la rendant programmable, reproductible et versionnable. Dans un contexte d’automatisation croissante des déploiements, les infrastructures doivent être définies, modifiées et déployées de manière fiable, rapide et sécurisée. IaC permet de réduire les erreurs humaines, d’assurer la cohérence entre environnements et de favoriser l’agilité des équipes techniques. Cet enseignement vise à doter l’élève ingénieur des fondements méthodologiques et techniques nécessaires pour concevoir, maintenir et sécuriser des infrastructures automatisées, au service de systèmes complexes et distribués.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Containérisation

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 ...)

- configurer un parc de machines virtuelles à l’aide de l’outil Ansible,
- Assimiler les notions fondamentales de cet outil : control host, targets, commandes ad hoc, modules Ansible, idempotence, playbooks, facts, rôles, etc.

Activités

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

- TD : 6 séances de 3h30
- Installation d’un cluster de machines virtuelles
- Exposé théorique des notions
- Nombreux ateliers pratiques pour l’assimilation par la pratique
- Exercices pour chacune des notions

Évaluations et retours faits aux élèves

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

Exercices en cours (contrôle continu)

INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-3 Infrastructure as code	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

<https://blog.microlinux.fr/formation-ansible/>