

## Pervasive Encryption on zOS

Durée: 3 Jours    Réf de cours: ESS10G

### Résumé:

In this course you will learn how to implement Pervasive Encryption in your z/OS installation. The course explores in detail, the various technologies that are involved in z System and z/OS Cryptographic Services, ICSF, RACF and DFSMS access method Services. In the hands-on exercises, you begin with the setup of your hardware crypto environment (CCA crypto express and CPACF), then you will load and activate your AES master keys, setup ICSF and its Key datasets (CKDS PKDS TKDS), then define your data encryption keys, activate your data set encryption policy, and encrypt your data sets and zFS filesystems. These exercises reinforce the concepts and technologies being covered in the lectures. This course consists of several inter-dependent modules. The modules, including the lab exercises, depend on the other previous modules content.

### Public visé:

This class is intended for z/OS system programmers and security specialists in charge of designing, implementing and monitoring Pervasive Encryption on z/OS.

### Objectifs pédagogiques:

- In this course, you will learn how to:
- Describe the components of Pervasive Encryption on z/OS
- Explain the role of encryption for data protection
- Implement hardware crypto on your z System
- Load and activate AES Master Keys
- Implement and start ICSF
- Understand the differences between secure keys clear keys and protected keys
- Describe how are key values used for encryption and decryption
- Generate, maintain and manage Keys
- Setup access to key labels
- Setup policy to supply key label (RACF SMS JCL)
- Access data in encrypted data sets
- Create encrypted data sets - Supplying key labels
- Convert existing data sets to encryption
- Verify encryption status
- Encrypt Data in Transit
- Encrypt Data at Rest
- Manage data sets, data keys, and key labels

### Pré-requis:

You should have the following prerequisites:

- General z/OS knowledge, including basic UNIX System Services skills
- Basic knowledge of RACF

### Test et certification

■

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

None

## Contenu:

### Day 1

- Welcome
- Unit 1: Pervasive Encryption Technical Foundation
- Unit 2: Pervasive Encryption: Planning
- Unit 3: Pervasive Encryption: implementation considerations
- Unit 4: Dataset Encryption Implementation steps

### Day 2

- Exercise 1: Setup and start ICSF
- Exercise 2: Load and initialize your AES master key and CKDS
- Unit 5: ICSF and crypto on z/OS
- Exercise 3: Define your data keys
- Exercise 4: Implement dataset encryption policy, encrypt/decrypt data sets

### Day 3

- Exercise 5: Operational tasks for managing data sets, data keys, and key labels
- Unit 6: Key management: ICSF and the Crypto Ecosystem on Z
- Unit 7: z15 Hardware Encryption Overview and Performance
- Exercise 6: Master Key Change using ICSF (optional)
- Exercise 7: Implement zFS encryption (optional)

---

## Méthodes pédagogiques :

Official course book provided to participants.

---

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

### Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)