

## Pervasive Encryption on z/OS

**Duration: 3 Days    Course Code: ESS10G    Delivery Method: Virtual Learning**

### Overview:

**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.

### Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

### Target Audience:

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

### Objectives:

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

### Prerequisites:

**You should have the following prerequisites:**

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

### Testing and Certification

None

---

#### Follow-on-Courses:

None

---

#### Content:

Please see the course objectives

---

#### Additional Information:

Official course book provided to participants.

---

#### Further Information:

For More information, or to book your course, please call us on 0800/84.009

[info@globalknowledge.be](mailto:info@globalknowledge.be)

[www.globalknowledge.com/en-be/](http://www.globalknowledge.com/en-be/)