

ICSF Programming Workshop (Course Code CRY80)

Create actual ICSF API flows and see the results!

4 Days Classroom; primarily Hands-on Labs

Scheduled dates:

February 6 - 9, 2001
May 15 - 18, 2001
August 14 - 17, 2001
November 6 - 9, 2001

Location:

Washington Systems Center
Gaithersburg, Maryland

Enrollment info:

US Call 1-800-IBM-TEACH
Outside US
Call 1-770-644-4475 or
E-mail rlundy@us.ibm.com

Description:

This 4-day hands-on workshop is designed to build skills in the coding of Integrated Cryptographic Service Facility (ICSF) APIs. This is done through lecture and coding exercises simulating a sample transactional flow typical to those used in ATM and POS environments. Learn by gradually building on concepts in the process of coding an ATM transaction on the host that communicates with a device simulator. Skills learned will be usable in non-financial environments as well.

No programming language skills are required. Teams of two will use a driver JCL interface and ICSF key management panels to perform exercises. The workshop is designed using a Driver that eliminates the need for the student to know a specific programming language and have coding skills. The workshop emphasizes the IBM Common Cryptographic Architecture (CCA) API concepts useful in programming with non-IBM and non-CCA IBM products. ICSF APIs are a subset of the IBM CCA APIs. Driver exercises will show ICSF API results without the need for application design or coding.

While the **focus** of the class is on the **coding of ICSF APIs**, attendees will also have opportunities to enter application keys into the Cryptographic Key Data Set (CKDS) using an ICSF utility. Both application programmers and key administrators will benefit from the material used. Usage and building of ICSF key structure and interaction with APIs is taught.

The workshop is a combination of lecture and hands-on lab with an emphasis on the hands-on lab. The lecture will provide the foundation knowledge of what is to be accomplished in the lab. The lab will implement the concepts described in the lecture and offer the opportunity to determine the depth of understanding and retention from previous exercises. Hints will be given to cause the student to think about WHY something is important.

Note: This workshop is not intended to teach basic concepts such as the key structure and usage within ICSF. This information can be learned by attending CMOS Cryptography & ICSF Implementation [ES80A]. However, the first day will contain an introductory lecture.

Who Should Take the Course:

Anyone who must use the IBM Common Cryptographic Architecture APIs to code applications using cryptography and anyone who must manage/inject application keys for use by cryptographic applications. ICSF and the software code supporting the IBM 4758 cryptographic hardware use IBM

Common Cryptographic Architecture and have a common set of APIs. This course is **very technical and requires basic knowledge** of cryptographic keys and concepts. This knowledge can be acquired by meeting the course prerequisites (see below). Knowledge of banking and ATM processing is not a requirement but this environment is used as the learning environment.

Special Notice:

Customers can use the driver to test or create API flows for their in-house applications during breaks and after they have completed the labs.

What You Are Taught:

- How to combine ICSF APIs to perform common functions used in lab exercises
- How to create keys received from systems that do not recognize the IBM CCA key structure
- How to create keys that can be used with systems not recognizing the IBM CCA key structures

Note: ICSF utility, KGUP, is used for key entry and will only be briefly covered to give you enough understanding to inject keys required by the exercises.

Audience:

Application Programmers interested in understanding how the ICSF APIs can be used and how to manipulate incoming keys for proper use in the IBM Hardware Crypto environment.

Application Key Administrators interested in understanding how the key functions within an application and what key types are required by the application programmers.

Crypto Architects interested in understanding how to interoperate between IBM crypto platforms and other crypto devices.

4758 Application Programmers on Netfinity (Windows NT), RS/6000, OS/400, Windows 2000, OS/2, and Windows NT Workstations.

Prerequisites:

- 1) ES80(A) or ES80(0) - ES80A is the course code for US; ES800 is the course code for Canada **or**

Working experience in crypto application or crypto application key entry. Experience does not have to be on ICSF.

- 2) Read ICSF Application Programmer's Guide, SC23-3976,
 - a) Chapter 1 - Data Encryption Standard (DES) Cryptography
 - b) Chapter 2 - Programming Considerations
 - c) Chapter 3 - Using the Callable Services
 - d) Appendix D - PIN Formats and Algorithms
 - e) Appendix F - Multiple Decipherment and Encipherment

Price:

\$2,000 US