IBM CCA/ICSF Course **Fall 2014**

This IBM CCA/ICSF Implementation Course familiarizes students with IBM's ICSF and its Common Cryptographic Architecture implementation. The course provides experience in configuring, programming, testing, and operating ICSF programs.

After participating in the course, students should be able to configure, program, and use ICSF in IBM Common Cryptographic Architecture (CCA) mode. In addition, participants should be able to design solutions that use IBM's other CCA products.

Description of the Course

Each student will learn how the ICSF and CCA products can be used to provide secure cryptographic functions for their unique applications. The instructors will show students how IBM ICSF and CCA can be used to provide a high-security cryptographic implementation. After completing the course, students should be able to implement cryptographic security techniques that use both symmetric and asymmetric algorithms with ICSF and to configure ICSF for maximum security.
In order to demonstrate and exercise CCA techniques, the classroom is equipped with a personal computer that has an IBM crypto card installed, so CCA concepts can be demonstrated easily.

The course includes:

- An introduction to general cryptographic concepts for information security
- The presentation of design objectives for the IBM Common Cryptographic Architecture
- Demonstrations and exercises of how to design and use cryptographic techniques that can be applied to information protection in real environments
- An emphasis on the implementation of security techniques using the ICSF product as a CCA cryptographic node, including the Crypto Express card for the IBM System z.
- Examples that teach students the design philosophy of programs that use DES or AES for data privacy and data integrity and RSA for digital signatures and symmetric key distribution.
  Note: Also the new ECC Diffie Hellman key distribution protocol will be explained and demonstrated.
- System programming details for ICSF and the inclusions of System SSL, z/OS Encryption Facility, IBM Tape Encryption and other standard solutions. The use of RACF the key rings and RACDCERT are also important in the tape encryption environment.

The first half of the class explores mainly the CCA aspects of the ICSF where the latter half of the class focuses more on the configuration and implementation of ICSF solutions on IBM System-z.

Who Should Take Part?

The course is designed for management and staff of IBM customers, system and application developers, and members of IBM organizations who are responsible for specifying and implementing cryptographic systems that use ICSF. The course is also beneficial for system designers, system analysts, system and application programmers, and security personnel.

The skills taught in this course are important for organizations such as banks, merchants, insurance companies, manufacturers, distributors, and governmental agencies that are involved with or employ e-commerce, automated teller machines, home banking, e-mail applications or need to implement data encryption. These organizations must safeguard their electronic communications and be able to prove to auditors that they have taken reasonable steps to protect their information.

The cryptographic techniques taught in this course can be used to protect information against misuse and ensure both the user's and the public's confidence in the system. During the course, students will learn the benefits of using IBM's CCA and its supporting applications to secure their organizations' information. Because of its high-security design and high performance, ICSF is the right choice for server systems. With software-only implementations of cryptography, cryptographic keys can be at risk. The IBM CCA hardware provides an essential, extra-measure of security for cryptographic keys as well as improved performance for popular public key techniques.

Course OUTLINE

DAY 1 (Monday)
- **Opening**
- **Basic Concepts of Symmetric Cryptography**

DAY 2 (Tuesday)
- **CCA Key Management**
- **Programming for the CCA API**
- **A Conceptual Overview of RSA**
- **The IBM PKA Implementation**

DAY 3 (Wednesday)
- **Cryptography overview & Implementation (ICSF based)**

DAY 4 (Thursday)
- **Cryptography usage on mainframes (ICSF based)**

DAY 5 (Friday)
- **Custom programming overview (UDX)**
- **Open questions and discussion (Greg and Andries)**
- **Closing of the Seminar**

For information, including related education seminars that run at customer's site, please contact Andries Mulder or Greg Boyd:

Mulder Training & Consultancy
Ir. Andries A.M. Mulder

The Netherlands
tel. +31 544 37 40 37 or +31 651 71 40 00
email: driesmulder@kpnmail.nl

MainframeCrypto.com
Greg Boyd

United States of America
tel. + 1 240 772 1539

email: gregboyd@mainframecrypto.com