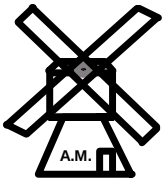

Mainframe Crypto, LLC

Mulder Training & Consultancy

ICSF Course

IBM CCA / ICSF IMPLEMENTATION Course

- for information purposes only -

2014/07/30

The 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.

Time, Place and Price

When: TBD

11:00 to 17:00 Monday
09:00 to 17:00 Tuesday - Thursday
09:00 to 13:00 Friday

Place: TBD

Price: 3,100 US$ per attendee for the whole week.

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**
- ✓ IBM's CCA implementation
- ✓ Symmetric and Asymmetric algorithms
- ✓ Cryptographic separation & initialization methods
- ✓ Requirement for cryptographic function isolation
- ✓ Cryptographic isolation via Control Vectors
- ✓ General IBM CCA Overview
- ✓ A Demonstration of the IBM CCA (by showing IBM 4765)

DAY 2 (Tuesday)

- **CCA Key Management**
- ✓ Generation of symmetric keys
- ✓ Master keys
- ✓ Where to store keys
- ✓ Backup considerations
- ✓ Distributing keys to remote nodes
- ✓ Exporting and importing keys
- ✓ Using key storage (CKDS)

- **Programming for the CCA API (T)**
- ✓ CCA calling conventions
- ✓ Compiling and linking application programs

- **A Conceptual Overview of RSA**
- ✓ Concepts of DES and PKA algorithms

- ✓ Application areas of PKA's
- ✓ Distributing symmetric keys using RSA
- ✓ Distributing symmetric keys using ECC Diffie Hellman
- ✓ Digital Signatures and non-repudiation

- **The IBM PKA Implementation**
- ✓ Generating key-pairs
- ✓ Importing and exporting keys
- ✓ Some CCA CSNDxxx verbs and their use

DAY 3 (Wednesday)

- **Cryptography overview & Implementation (ICSF based)**
- ✓ CCA Keys, CVs and Datasets
- ✓ ICSF Crypto Overview
- ✓ ICSF Crypto Implementation
- ✓ Crypto Microcode Loading Process
- ✓ Master Keys
- ✓ TKE concepts

DAY 4 (Thursday)

- **Cryptography usage on mainframes (ICSF based)**
- ✓ ICSF and other crypto users
- ✓ Key Generation Utility Program (KGUP)
- ✓ ICSF & SYSPLEX
- ✓ Application Programming
- ✓ ICSF & TKE implementation issues

DAY 5 (Friday)

- ✓ ICSF Logging & Performance (some examples)
- ✓ Misc information (Encryption Facility etc)

- **Custom programming overview (UDX)**
- ✓ User Defined Extensions
- ✓ Application Programming Examples

Open questions and discussion

Closing of the Seminar

This ICSF course is a joint project of Mainframe Crypto, LLC and Mulder Training & Consultancy. For more information on this course, or similar education offerings and sessions offered at the customer site, please contact Andries Mulder or Greg Boyd:

Mulder Training & Consultancy
Ir. Andries A.M. Mulder
tel. +31 544 37 40 37 or +31 651 71 40 00

Neptunus 19
7131 HN Lichtenvoorde
The Netherlands

email: driesmulder@kpnmail.nl
www.muldercrypto.com

MainframeCrypto.com
Greg Boyd
tel. + 1 240 772 1539

4307 Horine Ct.
Jefferson, MD 21755
United States of America

email: gregboyd@mainframecrypto.com
www.mainframecrypto.com

Bios:

Andries Mulder
Mulder Training & Consultancy is a one-man-company that is ran by Andries Mulder. Andries Mulder studied and graduated in Applied Mathematics at Twente Technical University in the Netherlands. In 1978 he joined IBM to work as a systems engineer working with System 36 and with other small business systems. When in 1980 the IBM PC was announced, he jumped into that new area and soon he was running courses on Pc Assembly language progamming and C-language programming. In 1989 IBM started a new exciting range of cryptographic products named TSS, Transaction Security System, the first product within the CCA (Common Cryptographic architecture) family of products. Since 1990 Andries ran several courses on IBM's crypto products and he continued to do so, after he left IBM for an early retirement.

Andries currently runs several classes on this family of IBM products and he is Authorized Service Provider for IBM 4764 and IBM 4765 Software Development Toolkit (UDX toolkits).

Greg Boyd
Greg is a Certified Information Systems Security Specialist (CISSP). Recently retired from IBM, Greg has started his own consulting firm, Mainframe Crypto, to provide consulting and technical assistance for implementing cryptographic solutions. Prior to leaving IBM, Greg spent the last 10 years providing technical marketing support for the System z Cryptographic hardware and software for IBM's Washington Systems Center. In that role, he assisted customers with installation and technical questions on the cryptographic products, and regularly presented at conferences such as SHARE, IBM's zTechnical University and the Vanguard Security and Compliance Conference.

ENROLLMENT FORM (please send to gregboyd@mainframecrypto.com

IBM CCA/ICSF Implementation Course	
Name of participant	
Company Name	
Address	
e-mail	
Purchase Order No. (if any)	
Name and Signature	

By enrollment the company agrees to pay US$ 3,100 that will be billed upon completion of the course.