Course Description

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR IMPLEMENTATION CLASS

Berlin, Germany, April 10 - April 14 , 2000

Presenters: Andries Mulder (IBM the Netherlands)

version 2000-02-18

The IBM 4758 Cryptographic Coprocessor Implementation Class familiarizes students with the IBM 4758 and its Common Cryptographic Architecture Support Program feature. The course provides hands-on experience in installing, programming, testing, and operating the IBM 4758.

After attending the course, students will be able to install, program, and use the IBM 4758 in its IBM Common Cryptographic Architecture (CCA) mode. In addition, participants will be able to design solutions that use IBM's other CCA products.

TIME, PLACE, COST

When — April 10th until April 14th, 2000
13:30 to 17:30 Monday
09:00 to 16:30 Tuesday-Thursday
09:00 to 13:00 Friday

Where — CSG Gmbh unternehmensbereich WBI
Alt-Moabit 101 A
10559 Berlin Germany
tel. +49-30-39076-500

Cost — DEM 4,900.00 (Deutschmark)

COURSE DESCRIPTION

Each student will learn how the IBM 4758 and CCA products can be used to provide secure cryptographic functions for their unique applications. The instructor will show students how the IBM 4758 and its CCA Support Program feature can be used to provide a high-security cryptographic implementation. After completing the course, students will be able to implement cryptographic security techniques using the IBM 4758 in mixed DES and RSA environments and to configure the Coprocessor for maximum security.

The classroom is equipped with personal computers that have the IBM 4758 installed.

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 IBM 4758 product as a CCA cryptographic node
- Examples that teach students the design philosophy of programs that use DES for data privacy and data-integrity and RSA for digital signatures and symmetric key distribution.

The first half of the class explores the access control and DES aspects of the IBM 4758 CCA product. The latter half of the class focuses on the use of RSA techniques and integration of the IBM 4758 with other IBM products. The course is conducted in a special classroom that is equipped for hands-on training.

WHO SHOULD ATTEND

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 the IBM 4758. 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 in or employ E-Commerce, automated teller machines, home banking, and e-mail applications. These organizations must safeguard their electronic communications and be able to prove to auditors that they have taken all 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 the IBM 4758 and its supporting applications to secure their organizations' information. Because of its high-security design, the IBM 4758 is the right choice for server systems. With software-only implementations of cryptography, cryptographic keys can be at risk. The IBM 4758 provides an essential, extra-measure of security for cryptographic keys as well as improved performance for popular public key techniques.

COURSE LANGUAGE

The course will be taught in English.

ENROLLMENT

You can enroll by providing the listed information through e-mail or fax (fax preferred) to:

Ms. Angela Wenemoser
csg Computer Service GmbH
...an IBM global services Company
Kaiserswertherstr. 119
Düsseldorf, Germany

wenemos@de.ibm.com (Internet)
Angela Wenemoser/Germany/IBM@IBMDE (Internal)

Telefon: +49 211 476 1408
Fax: +49 211 476 2764

Note that seats are limited due to the hands-on nature of this class; enroll early.

Enrollment Information

Participant name and title
Company name
Company or department description
Full business address
IBM Customer Number
Telephone number
Fax number

No enrollment confirmations will be sent until 10 days before the planned start date of the class. If you require an earlier confirmation, please contact Andries Mulder. The class is subject to cancellation in the event of inadequate enrollments; we would appreciate your early enrollment.

Payment Details

The fee for the course is DEM 4,900.00 excluded VAT.

Hotel Accommodations

The CSG/IBM Education Facility is located in the center of Berlin
Make hotel accommodations through your travel representative.
Hotel and meal expenses are not included in the course fee.
A few hotels that are not too far from the course location are listed below:

- Hotel Park Consul Berlin tel. +49-30-390-780
  (on Alt Moabit on walking distance)
- Hotel Tiergarten
  (on Alt Moabit on walking distance)
- Hotel Excelsior
  (Hardenbergerstrasse near Kurfurstendamm, 2 stops with subway)
- Forum Hotel Berlin tel. +49-30-23890
  (Alexanderplatz, 4 stops with subway)
- Hotel Unter den Linden
  (Unter den Linden, 3 stops with subway)

Alternative Courses

It is our intention to run this class on a regular basis in Europe and in Charlotte USA.
In case that more than 3 to 4 attendees from one country or customer are to attend this course, it may be more cost efficient to give a special customer tailored course on site. (e.g. at customers location). In this case the course can be customized more to specific customers requirements (eg. more or less programming materials, CCA on AS/400 etc.
Also interpreter services can be easier implemented in such a course.
For more information contact Andries Mulder (see address information at the end of this document)

COURSE OUTLINE

(T) = Theory (P) = Practice

DAY 1 (Monday)

- **Opening** (T)

- **Basic Concepts of Symmetric Cryptography** (T)
  - ✓ IBM's CCA implementation
  - ✓ Configuration examples
  - ✓ Cryptographic separation & initialization methods
  - ✓ Requirement for cryptographic function isolation
  - ✓ Cryptographic isolation via Control Vectors.
  - ✓ General IBM 4758 Overview (T)

- **A Demonstration of the IBM 4758** (T+P)

DAY 2 (Tuesday)

- **Installing and Customizing an IBM 4758** (T)
  - ✓ Concepts of customizing an IBM 4758
  - ✓ The Crypto Node Management Utility (CNM) installation
  - ✓ How to use the Node Management Utility.

- **Loading the System Software into the IBM 4758** (T)
  - ✓ Loading the software
  - ✓ Feature Control Vectors, and how to load them.

- **Access Control in the IBM 4758** (T)
  - ✓ Roles
  - ✓ Profiles
  - ✓ Logon and its Context.

- **Installing and Customizing an IBM 4758** (P)
  - ✓ Using the CNM-utility
  - ✓ Testing the DEFAULT role
  - ✓ Loading other roles
  - ✓ Loading profiles
  - ✓ Setting Data and Time
  - ✓ Customizing with a user program

DAY 3 (Wednesday)

- **CCA Key Management** (T)
  This presentation gives a more detailed discussion on the concepts of cryptographic key-handling in CCA programs.
  - ✓ Generation of keys
  - ✓ Where to store keys
  - ✓ Backup considerations
  - ✓ Distributing keys to remote nodes
  - ✓ Exporting and importing keys
  - ✓ Using key storage.

- **Programming for the CCA API (T)**
  - ✓ CCA calling conventions
  - ✓ Compiling and linking application programs
  - ✓ Some CCA verbs and their use
  - ✓ CCA return codes and reason codes
  - ✓ CCA pseudo code samples
  - ✓ Running CCA programs with Easy58.

- **Testing CCA designs with EASY58 (T+P)**

DAY 4 (Thursday)

- **Setting Up a Symmetric Key Management System** (T)
  In this presentation an example of a real-life key-management-center application based in CCA cryptography is discussed. The programs required on the center and user-nodes are presented using pseudo code so that the ideas behind the actual programs become clear.

- **A Conceptual Overview of RSA** (T)
  - ✓ Concepts of DES and PKA algorithms
  - ✓ Application areas of PKA's
  - ✓ The N-Square problem and the solution to that
  - ✓ Initial DES key distribution
  - ✓ Digital Signatures and non-repudiation

- **The IBM PKA Implementation** (T)
  Generating key-pairs
  Importing and exporting keys
  Some CCA CSNDxxx verbs and their use
  How to use a certification center.

- **Initial DES Key Distribution** (P)
  A case study presentation of a DES key distribution system with the use of public key cryptography demonstrates the use and capabilities of the IBM 4758 CCA implementation.

- **Digital Signature Case Study**
  In this case study presentation, all the steps required to generate and verify digital signatures between two nodes in a network are examined.
  - ✓ Explanation of the steps in the process
  - ✓ Running the programs.

DAY 5 (Friday)

- **A Positioning of the S/390 CMOS Crypto feature and the IBM 4758 (T)**

- **Master Key Cloning and How to Use It** (T)

- **CDSA and Keyworks**

- **Custom programming overview:** (T)
  User Defined Extensions
  The Custom Programming Toolkits

- **New models of the 4758** (T)
  Hardware changes
  New Software (PKCS #11)

- **Closing of the Course**

TOPICS OF RELATED COURSE OFFERINGS

On request, course(s) that cover these topics can be quickly offered:

- Securing Workstations in a Practical Way (T)
- Installation and Customization of 4753 NSP (T)
- CCA on the RS/6000 (T)
- CCA on the AS/400 (T)
- PKA92 for TSS, the first CCA RSA implementation (T+P)

For information about these related classes or for information about courses that run at customers site, please contact Andries Mulder:

ir. Andries A.M. Mulder
IBM Nederland NV
PO Box 9999
1006 CE AMSTERDAM
The Netherlands
tel.+31-20-5134776 or tel.+31-653-763989 or tel.+31-544-374037
fax +31-544-374969
email: andries_mulder@nl.ibm.com or driesmul@wxs.nl
IBM Notes -address: Andries AM Mulder/Netherlands/IBM @ IBMNL

Snail-mail and FAX Enrollment Form

IBM 4758 PCI Cryptographic Coprocessor Implementation Class, AP058

Name and Title of Participant:. . . . . .

Company Name: . . . . . .

IBM Customer number . . . . . .

Full address: . . . . . .

City: . . . . . .

Country: . . . . . .

Tel. number:. . . . . .

Fax number: . . . . . .

e-Mail: . . . . . .

IBM Customer Number: . . . . . .

Hereby I declare that I / My company will
pay the course amount of DEM 4.900,-- (plus VAT)

Signature _____

Please Send or Fax to Ms. Angela Wenemoser
csg Computer Service GmbH
...an IBM global services Company
Kaiserswertherstr. 119
Düsseldorf, Germany

wenemos@de.ibm.com (Internet)
Angela Wenemoser/Germany/IBM@IBMDE (Internal)
Tel.: +49 211 476 1408
Fax: +49 211 476 2764

After sending the fax to mrs Wenemoser, please send an e-mail or make a phone call to verify the proper transmission.