fit for mainframe

Cryptography und Mainframe Hardware Support

für

- **Systemprogrammierer**
- **systemorientierte Mitarbeiter**

Version 1.7 vom Juli 2021

Autor: Wolfram Greis

European Mainframe Academy GmbH
Am Klostergarten 3
D 78337 Öhningen
Tel. +49-7736-938 8668
ann-chatrine.mueller@mainframe-academy.de

European Mainframe Academy AG
Obergass 23
CH 8260 Stein am Rhein
Tel. +41-52-558 20 40
wolfram.greis@mainframe-academy.de

Inhaltsverzeichnis

1 Ziele des Ausbildungsmoduls

2 Informationen zum "Blended Learning" der EMA

Die Lehrgangsmodule der EMA sind eingeteilt in Pflichtstoff und Wahlstoff. Der Pflichtstoff ist prüfungsrelevant, d.h., dass die entsprechend vermittelten Kenntnisse in Tests, Prüfungen und praktischen Arbeiten vorhanden sein müssen und abgefragt werden, falls am Ende des Moduls ein Zertifikat erlangt werden soll.

Der Wahlstoff kann auf freiwilliger Basis durchgearbeitet werden. Selbstverständlich stehen für sämtliche Belange qualifizierte Fachkräfte für die Beantwortung von Fragen zur Verfügung.
Der durchschnittliche Lernaufwand für den Pflichtstoff beträgt ca. 10 Stunden pro Woche.

Die Module bestehen aus:

- Virtuelle Klassenzimmer Sessions
- E-Learning
- Theoretische und praktische Übungen

3 Inhaltsbeschreibung

Im Folgenden werden die Module detailliert beschrieben.

3.1 Kick-off

Kick-off
Mit diesem Kick-off wird die Basis einer erfolgreichen Zusammenarbeit während der gesamten Lernphase gelegt.

Dauer: 2 Virtual Classroom Sessions

Datum s. Starttermine

Ort Virtuell

Ziele des Kick-offs Mit diesem Kick-off sollen drei Dinge erreicht werden:

- Die Teilnehmer und die Key-Dozenten lernen sich gegenseitig kennen
- Die Teilnehmer lernen die wichtigsten E-Learning Werkzeuge kennen, vor allem das Virtuelle Klassenzimmer
- Die Teilnehmer bekommen einen ersten Überblick über die Seminarinhalte

Inhalt

Einführung
Vorstellungsrunde
Einführung in das Thema

Lerneffizienz
Lernen und Erkenntnisse der Neurobiologie
Effizientes Lernen

E-Learning & Blended Learning
Der Bedeutung von E-Learning
Die Vorteile des Blended Learning
Integration von Web 2.0
E-Learning Werkzeuge im Überblick

Lernplattform Moodle
Übersicht über die Lernplattform
Aufbau der Lernplattform

Das Virtuelle Klassenzimmer
Ziele einer VC-Session
Unterschiede zum herkömmlichen Klassenzimmer
Einsatz des Virtuellen Klassenzimmers

Zugriff auf den Mainframe
Die Infrastruktur der EMA
Zugriff auf den IBM Rechner

Security Einführung
Anforderungen
Verschlüsselungstechniken
Gruppenarbeit

3.2 Verschlüsselungstechniken

Ziele dieses Untermoduls
Die Teilnehmer kennen die Verschlüsselungstechniken und deren historische Entwicklung bis in das Computer- und Internet-Zeitalter. Sie kennen den Unterschied zwischen symmetrischen und asymmetrischen Techniken sowie deren Vor- und Nachteile. Sie können die Unterschiede zwischen DES, RSA und AES erklären.

Inhalt

Historie der Verschlüsselung von Informationen
Mesopotamische Tontafel
Caesar`s Verschiebealgorithmus

Kryptologie / Kryptographie / Kryptoanalyse
Terminologie und Begriffe
Kryptografische Algorithmen
Kryptografische Protokolle
(Private Key / Public Key Verfahren)
Sicherheit von Schlüsseln

Arten von Chiffren
Klassische Chiffren
Blockchiffren (DES, AES)
Public-Key-Kryptographie

Authentifikation und digitale Signatur
Einwegfunktionen
Zero-Knowledge-Protokolle
Digitale Signaturen

Public Key Kryptographie
RSA Algorithmus und Implementierung
Algorithmen und Elliptische Kurven

Public Key Infrastruktur (PKI)
Prüfung öffentlicher Schlüssel
Trustcenter (CAs)
Zertifikatshierarchie
Web-of-Trust

Public Key Systeme
Pretty Good Privacy (PGP)
S/MIME und das X.509 Protokoll
Secure Shell (SSH)
SSL und TLS
IP Security und VPN

Elektronische Systeme
Elektronisches Bargeld
Elektronische Zahlungssysteme

Gesetzliche Rahmenbedingungen
Deutsche und Europäische Regelungen
US Exportgesetze

3.3 System z Hardware Kryptographie

Ziele dieses Untermoduls
Die Teilnehmer kennen die kryptographischen Möglichkeiten, die in der IBM Hardware z10, 196, z114 und zEC12 eingebaut sind und wie diese mit der ICSF (Integrated Cryptographic Service Facility) Komponente des z/OS zusammenarbeiten.

Sie kennen die zur Verfügung stehenden APIs und dien Interaktionen mit dem z/OS Security Server (RACF) und die Schlüsselverwaltung.

Ebenfalls behandelt werden die Möglichkeiten in Verbindung mit Trusted Key Entries (TKE) und das Distributed Key Management System (DKMS).

Inhalt

Integrated Cryptographic Service Facility
Infrastruktur und Implementation
IBM CCA (Common Cryptographic Architecture) API
Key Management mit ICSF

Performance Considerations

Augmented SAF/RACF Protection

ICSF Installation & Customization
Installation von ICSF
Anpassung an die eigene Umgebung
ICSF Administration

Die optionale TKE Workstation

Die optionale DKMS Workstation