

**Course Title:**

Secure Electronic Commerce

**Course Designator/Course Number:**

IAF-SEC

**Course Description**

In this course, the student will learn about the history, present, and future of electronic commerce in the world. The student will also learn about the threats, vulnerabilities and policies when dealing with commerce in the electronic age.

**Course Prerequisites:**

- Principles of Information Assurance
- Network Security
- Enterprise Security Management

**Course Length:**

90 contact hours in 3-hour sessions for a 6-week duration.

**Required Texts:**

- Security Certified Program (SCP) curriculum:  
Enterprise Security Solutions  
Warren Peterson; Uday O. Ali Pabrai.  
ISBN: 0-7580-7481-6

**HTTP Link:**

<http://security.ctln.org/SEC>

## Course Learning Topics and Objectives:

There are 9 exams covering these topics and objectives, a final exam and a hands-on performance final. Upon completion of these modules, students will be able to perform tasks related to:

1. Secure E-Commerce Concepts & Practices: In this topic, the core concepts that comprise secure e-commerce are explored. The most common practices used today are examined.

### Objectives:

- a. Define E-Commerce and identify the key components.
  - b. Examine the history of E-Commerce and how E-commerce integrates into the economy.
  - c. Examine the common methods used in E-Commerce.
  - d. Explore the security risks associated with E-Commerce.
  - e. Examine how E-Commerce is included in security policies.
  - f. Explore current and future trends in E-Commerce practices.
2. Trusted Network Implementation: In this topic, you will examine and identify the transition towards the implementation of trusted networks, including their requirements and critical components.

### Objectives:

- a. Examine reasons for migrating networks from defense to trust.
  - b. Analyze the requirements of a trusted network.
  - c. Define the fundamentals of cryptography.
  - d. Define the role of strong authentication.
  - e. Define the role of a public key infrastructure.
3. Planning a Trusted Network: In this topic, you will be introduced to the concepts and documents required in planning a trusted network. You will examine trusted network architectures, certificate paths, certificate policies, certification practice statements, and the certificate policy framework.

### Objectives:

- a. Examine the components required for a trusted network implementation.
- b. Analyze certificate paths.
- c. Analyze trusted network planning documents.
- d. Examine the certificate practices framework.

4. Microsoft Trusted Networks: In this topic, you will examine the requirements for Certificate Authorities (CA) in general and the various models of CAs that are implemented in practice. You will study the key elements that have to be in place in order for a Certificate Authority to have any meaning for the organization it is designed to serve.

Objectives:

- a. Examine the requirements surrounding the implementation of a CA.
  - b. Examine the critical function that trust plays between CAs in a network built on trust.
  - c. Examine the types of certificates in a trusted network.
  - d. Implement a standalone Microsoft Certificate Authorities hierarchy.
  - e. Implement a Microsoft Enterprise Root CA.
5. Linux Certificate Authorities: In this topic, you will examine the basics of certificate authorities on Linux.

Objectives:

- a. Examine the requirements for implementing Certificate Authorities on a Linux platform.
  - b. Examine multiple CA options on Linux.
  - c. Prepare a Linux server for a CA implementation.
  - d. Examine the fundamentals of LDAP.
  - e. Install and configure a Linux CA package.
6. Managing Certificates: In this topic, you will examine issues related to the management of certificates. Depending upon the size of the organization and depending upon whether the CA is hosted internally or not, certificate issuance policies may vary.

Objectives:

- a. Examine the management of certificates base on end entity needs.
- b. Create certificate requests and use a CA to generate the certificates for computers and users.
- c. Issue multiple types of digital certificates.
- d. Assign the issued certificate to the entity that requested it.
- e. Implement certificates on smart cards.

7. Local Resource Security: In this topic, you will examine multiple systems and technologies available to secure data stored locally on your computer.

Objectives:

- a. Examine how Windows operating systems function.
  - b. Configure Windows Encrypted File System (EFS).
  - c. Configure a system to prevent users from using EFS.
  - d. Implement EFS to protect files.
  - e. Implement data security using biometrics.
8. Secure Email: In this topic, you will examine the current vulnerabilities of email and the reasons that plaintext is a serious security risk for any enterprise.

Objectives:

- a. Examine the benefits and challenges of secure email.
  - b. Implement PGP (Pretty Good Privacy) to secure email.
  - c. Implement S/MIME to secure email.
  - d. Explore other options to secure email.
9. Building Trusted Networks (Lab Only): In this topic, you will take the different pieces that you have worked with through the course and tie them together in a simulated environment.

Objectives:

- a. Implement a multi-platform CA structure.
- b. Configure the CA hierarchy.
- c. Configure the Linux CA.
- d. Implement trusting CAs.
- e. Implement multi-platform secure email.
- f. Revoke certificates and verify revocation.