Introduction to FIPS 140-2

Duration:

1/2 day

Audience:

This course is aimed at development team members who will be involved in a FIPS 140-2 evaluation.

Prerequisites:

Basic knowledge of product development life cycle

Course Goals:

After completing this course, the trainee will have the knowledge and skills to:

- Understand why FIPS 140-2 certification is mandatory
- Understand the Crypto Module Validation Program
- Understand Cryptographic Modules
- Understand testing requirements

Course Outline:

- Knowledge of FIPS history
  - FISMA
- Knowledge of the Cryptographic Module Validation Program (CMVP)
- General knowledge of the validation process
- Knowledge of Cryptographic Modules
  - Security Functionality
  - Cryptographic Boundaries
  - Security Objectives
- General knowledge of the overall FIPS 140-2 standard structure
  - Key Documents
- Ability to understand security functional areas
  - Knowledge of Security Levels
  - Knowledge of EMI/EMC compliance
- Knowledge of Derived Test Requirements (DTR)
- Understanding of Cryptographic Algorithm Validation Process