

Security & Cryptography

Objectives:

At the end of this course you will:

- ✦ Understand smart card security, smart card oriented cryptography and related issues

Key Topics:

- ✦ Basics of security and cryptography
- ✦ Key management
- ✦ Open OS card security
- ✦ Side channel attacks
- ✦ SPA attacks
- ✦ DPA attacks
- ✦ DFA attacks
- ✦ Fraud control

Who should attend:

- ✦ R&D personnel
- ✦ - to implement cryptographic procedures
- ✦ - to take smart card cryptographic aspects into account



Cryptography is the science of secure communication. In addition to providing confidentiality, cryptography provides authentication, integrity & non repudiation. Gemalto has a long history and recognised expertise in cryptography-based solutions around smart cards.

This training seminar will allow you to benefit from this experience

Each training session consists of:

- ✦ A complete course manual

Pre-requisites:

- This course requires participants to have a basic knowledge in hardware and software development, mathematics and computer science
- ✦ This course is held in English

Duration: 3 Days

Course fee:

Please refer to regional schedules on www.gemalto.com/training or contact us: <http://www.gemalto.com/training/contact.html>

Location:

Gemalto Training Centers. For on-site training, please contact us.

Course Schedule:

Day 1

Welcome and training overview

FOUNDATIONS

- + Information Security
- + Cryptography Basics
- + Common cryptographic protocols
- + Key Management
- + PKI Overview
- + ISO-15408 standard: Common Criteria

Day 2

SMART-CARDS AND SECURITY

- + Introduction to Smart Card
- + Invasive Attack
- + Side Channel Attack
- + SPA Attacks and counter measures
- + DPA Attacks and counter measures
- + DFA Attacks and counter measures

Day 3

OTHER SECURITY ASPECTS

- + Smart Card Fraud Control & Real Life Scenario
- + GSM-3G security
- + Secure programming techniques overview
- + Smart Card Security : managing the risks
- + Overall conclusion