

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
- + ISO-15408 standard: Common Criteria
- + Open Card OS Security

Day 2**SMART-CARDS AND SECURITY**

- + Introduction to Smart Card
- + Side Chanel Attack
- + SPA Attacks and counter measures
- + DPA Attacks and counter measures
- + DFA Attacks and counter measures
- + Demos if possible

Day 3**OTHER SECURITY ASPECTS**

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

Presentations done during the third day can be adapted to the client's need and background.

Related Courses:

**Security &
Cryptography
(S10012)**

**PKI Fundamental
of Secure
Networking
(S1001S)**