UNIVERSITY OF LONDON | INTERNATIONAL PROGRAMMES

Royal Holloway University of London

## University of London International Academy
## MSc/PG Dip in Information Security
## Lead College – Royal Holloway

# Smarty Cards/Tokens Security and Applications IYM012 (Option)

### Aims

This course will:

- provide an overview of smart cards/tokens and their properties
- introduce various applications that exploit smart cards/tokens
- examine benefits, threats and attacks
- consider systems for the development, manufacture and management of smart cards/tokens
- review smart card standards and security evaluation methodologies

### Pre-requisites

None

### Essential Reading

- Smart Cards, Tokens, Security and Applications (K.Mayes, K.Markantonakis) Springer, Science & Business Media-2008

Included as study material once registered on the course.

### Assessment

This module is assessed by a two hour unseen written examination.

### Learning Outcomes

On completion of this module students will be able to:

- identify constituent components, analyse strengths and weaknesses and identify new applications of smart cards
- identify the steps in the manufacturing/personalisation processes, analyse and evaluate potential risks and compare security safeguards
- identify and compare the systems in use, analyse the strengths and weaknesses and evaluate interoperability and security issues
- analyse the range of capabilities of SIM/USIM cards and apply them to new service ideas, evaluate the possible range of services and security measures
- understand the main standards and applications of smart cards for banking and finance, compare with earlier card solutions and analyse strengths and weaknesses of approaches
- analyse the key role of the smart card for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards
- identify and describe new technologies, including TPMs and apply them to new applications and evaluate the likely suitability/success of approach
- explain how Common Criteria may affect smart card design/development, analyse the different approaches and compare with less formal methods
- identify and describe the classes of attack and notable methods within each class, analyse countermeasures and evaluate practicality of attacks

- identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools
- analyse the issues concerning smart card lifestyle management, and evaluate and compare methods of local and remote card management

## Syllabus

***Unit 1*- An Introduction to Smart Cards**
Unit 1 is based on the presentation **“”** by Dr Keith Mayes of the Information Security Group Smart Card Centre (ISG SCC). This unit leads the students through an introduction to the basics of smart card related issues. It reviews the different types of cards and token platforms along with introducing the main types of popular smart card applications. The presentation aims to motivate and provide context for the rest of the units.

***Unit 2*** – **Trusted Production Environment**
In Unit 2, Wolfgang Rankl (Giesecke & Devrient) presents various issues associated with the smart card production chain. The unit examines the processes (e.g. production of the card body, chip moulding, personalisation and card delivery) involved in smart card production

***Unit 3*** -**An Overview of Multi-Application Smart Card Platforms**
is delivered by Dr Konstantinos Markantonakis (ISG SCC). Having examined the basic functionality of smart card technology in the previous two modules, this presentation provides an overview of the most widely utilised multi-application smart card platforms.

***Unit 4*** - **SIM/USIM Cards, Applications & Security for Mobile Telephony”**
The mobile telecommunications industry utilises more smart cards than any other sector. This unit is delivered by Tim Evans (Vodafone). He discusses the role of the SIM and USIM in the mobile telecommunications industry. At the same time he reviews the evolution of smart cards, GSM standards and other technologies (such as the SIM Toolkit) as the main building blocks for offering enhanced and secure services in the telecommunication industry.

***Unit 5*- “Information Security & Crypto @ Visa”**
is delivered by David Main (Visa) and Dr Karl Brincat (Visa). The presentation examines how cryptography and various other technologies (e.g. cards, tokens, 3D secure) are utilised by a financial institution like Visa International.

***Unit 6*** comprises of two different presentations:
In Unit 6a,**“ID Cards and Passports”**
Ingo Liersch (Giesecke & Devrient) examines the recent proposals and standards related with the utilisation of secure tokens for the provision of e-passport and e-ID applications. The presentation also covers issues around biometrics and how they affect any proposed solutions.

***Unit 6b,* “Security For Video Broadcasting”**,
Dr Allan Tomlinson (ISG) examines various issues around the protection of digital content in the satellite TV industry. In particular, he examines how smart card technology is utilised as the main security mechanism for the protection of the transmitted content.

***Unit 7* -**Unit 7 is composed of two distinct presentations:
Unit 7a-**Trusted Platform**
Dr Allan Tomlinson (ISG) provides an overview of the Trusted Production Module (TPM) and highlights how it compares with smart cards in terms of technology, overall architecture, management and ownership.

*Unit 7b*-**Advances in Chipcard Technology**
Chris Shire (Infineon) examines the past and the future of smart card technology. It highlights issues around the future of smart card chips by taking into account various limitations in terms of size, processing power, and cost. Finally, he discusses issues around consumer demand.

***Unit 8*** **- Evaluating Smart Card Security with the Common Criteria**
Tony Boswell (Siventure).This unit explains how Common Criteria has evolved and how it is applied in practice to the complex and highly demanding field of smart card security evaluations.

***Unit 9*** **- Security Attacks, Countermeasures and Testing for Smart Cards**
Jacques Fournier (Gemalto) focuses on the wide range of smart card security attacks and countermeasures that need to be considered when planning commercial smart card offerings.

***Unit 10*** **- *A*pplication Development Environments for Java and SIM Toolkit**
Gary Waite (O2) presents an overview of the wide range of issues associated with the smart card application development process. More specifically he examines Java Card, SIM and USIM applications.

***Unit 11*** - **OTA and Secure Lifecycle Management** is delivered by Rudolf Oswald (Swisscom) and Joos Cadonau (Sicap). They explore how smart card technology is managed within the telecommunications industry. More specifically, they examine how the mobile phone operators are utilising the necessary tools to perform Over-The-Air (OTA) updates and deliver content to mobile devices.