INFORMATION SECURITY GROUP
Course Specification 2013-14

Code:	IY5606	**Course Value:**	0.5	**Status:**	Option
Title:	**Smart Cards/Tokens Security and Applications**			**Availability:**	Spring Term
Prerequisites:	Core courses			**Recommended:**	None
Co-ordinator:	Keith Mayes				
Course Staff	Keith Mayes plus invited ISG and industry experts				
Aims:	This course will: • provide an overview of smart cards/tokens/RFIDs and their properties • introduce various applications that exploit smart cards/tokens/RFIDs • examine benefits, threats and attacks when used as assets for Cyber Security • consider systems for the development, manufacture and management of smart cards/tokens/RFIDs • review smart card standards and security evaluation methodologies				
Learning Outcomes:	On successful completion of the course students will be able to: • identify constituent components, analyse strengths and weaknesses, identify new applications of smart cards/security tokens and their use as assets in cyber security • 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 in Smartphones 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/RFID for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards, • identify and describe new technologies, including NFC, TPM, TEE; 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 and the effects on cyber security • 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 lifecycle management, and evaluate and compare methods of local and remote card management				
Course Content:	1. Introduction to Smart Cards/Chips & RFID/NFC; Assets for Cyber Security 2. Smart Cards – Trusted Production Environment 3. Operating systems, Interoperability and Security 4. Applications & Security for Mobile Communications, USIM/SIM, Services and Clouds 5. Smart Cards for Secure Banking & Finance 6. Smart Cards in eIDs/Passports - & RFIDs/NFC explained 7. Advances in Smart Chips/Tokens, and Transport System Case Study 8. Common Criteria and Smart Cards 9. Security Attacks, Countermeasures and Testing for Smart Cards/RFIDs/NFC 10. Application Development Environments for JAVA and SIM Toolkit 11. Comparing Alternative Security Tokens/Environments; including TPM and TEE				
Teaching & Learning Methods	Lectures delivered by industry experts & ISG-SCC staff, Some practical demonstrations Private study: Students are encouraged to read the course text book and review international standards				
Key Bibliography:	Course Text book: Keith Mayes, Konstantinos Markantonakis, "Smart Cards, Tokens, Security and Applications", Springer-Verlag New York, January2008, ISBN: 0387721975 W. Rankl and W. Effing – "Smart card handbook" 2nd edition John Wiley 1997 Klaus Finkenzeller, "The RFID Handbook", John Wiley and Sons 2003 Zhiqun Chen, "Java Card Technology for Smart Cards", Addison- Wesley 2000. Keith Mayes, Konstantinos Markantonakis, "Secure Smart Embedded Devices, Platforms and Applications", Springer-Verlag New York, 2013, ISBN 978-1-4614-7914-7				
Formative Assessment and Feedback:	There are formative feedback quizzes that are set within one lecture and answered at the following lecture. There are also sample questions/problems that the student may optionally answer. Feedback is given at the lectures, via e-mail and sometimes one-to-one as requested by the student.				
Summative Assessment	**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. *(3 out 5 questions)* **Coursework** 0(%) Coursework does not contribute to the final assessment for this course. **Deadlines:** The written examination will be held in the Summer term				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.