

# Table of Contents

## Invited Talk

Protecting Consumer Security Devices (The Next 10 Years) .....	1
<i>Simon Moore</i>	

## Contributed Papers

Jakarta: A Toolset for Reasoning about JavaCard .....	2
<i>G. Barthe, G. Dufay, M. Huisman, and S. Melo de Sousa</i>	
Mechanising a Protocol for Smart Cards .....	19
<i>Giampaolo Bella</i>	
JCCM: Flexible Certificates for Smartcards with Java Card .....	34
<i>Celeste Campo, Andrés Marm, Arturo García, Ignacio Díaz, Peter T. Breuer, Carlos Delgado, and Carlos García</i>	
Context Inference for Static Analysis of Java Card Object Sharing .....	43
<i>Denis Caromel, Ludovic Henrio, and Bernard Serpette</i>	
Automated Test and Oracle Generation for Smart-Card Applications .....	58
<i>Duncan Clarke, Thierry Jéron, Vlad Rusu, and Elena Zinovieva</i>	
An Internet Authorization Scheme Using Smart-Card-Based Security Kernels .....	71
<i>Yves Deswarte, Noredine Abghour, Vincent Nicomette, and David Powell</i>	
Turning Multi-applications Smart Cards Services Available from Anywhere at Anytime: A SOAP/MOM Approach in the Context of Java Cards .....	83
<i>Didier Donsez, Sébastien Jean, Sylvain Lecomte, and Olivier Thomas</i>	
An Operational Semantics of the Java Card Firewall .....	95
<i>Marc Éluard, Thomas Jensen, and Ewen Denne</i>	
CardS4: Modal Theorem Proving on Java Smartcards .....	111
<i>Rajeev Prabhakar Goré and Phuong Thê Nguyễn</i>	
iButton Enrolment and Verification Requirements for the Pressure Sequence Smartcard Biometric .....	124
<i>Neil J. Henderson, Neil M. White, and Pieter H. Hartel</i>	
SIMspeak – Towards an Open and Secure Application Platform for GSM SIMs .....	135
<i>Roger Kehr and Hendrik Mieves</i>	

VIII Table of Contents

On-Card Bytecode Verification for Java Card .....	150
<i>Xavier Leroy</i>	
Towards a Full Formal Specification of the JavaCard API .....	165
<i>Hans Meijer and Erik Poll</i>	
Protection Profiles and Generic Security Targets for Smart Cards as Secure Signature Creation Devices – Existing Solutions for the Payment Sector .....	179
<i>Gisela Meister and Michael Vogel</i>	
A Flexible Invocation Framework for Java Card .....	188
<i>Michael Montgomery and Ksheerabdhhi Krishna</i>	
ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards .....	200
<i>Jean-Jacques Quisquater and David Samyde</i>	
Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm .....	211
<i>Tanja Römer and Jean-Pierre Seifert</i>	
Use of Biometrics for User Verification in Electronic Signature Smartcards .....	220
<i>Bruno Struif</i>	
Programming Internet Smartcard with XML Scripts .....	228
<i>Pascal Urien</i>	
Public-Key-Based High-Speed Payment (Electronic Money) System Using Contact-Less Smart Cards .....	242
<i>Hideo Yamamoto, Tetsutaro Kobayashi, Masahiro Morita, and Ryuji Yamada</i>	
<b>Author Index</b> .....	255