



PROCEEDINGS
OF THE FIRST SMART CARD
RESEARCH
AND
ADVANCED APPLICATION
CONFERENCE

V. Cordonnier J-J. Quisquater (Eds)

Sponsored by IFIP

October 24 - 26, 1994
LILLE—FRANCE



Contents

Session 1 : Security

Making smartcard systems robust	1
Ross Anderson (UCL, Cambridge)	
The RADAR concept using neural networks	15
T. Alexandre (RD2P, Lille)	
A security language for the card: The S-shell	33
J.-M. Place and P. Trane (RD2P, Lille)	

Session 2: Panel

Future operating systems for smart cards?
Moderator: Philippe Maes (Gemplus)

Session 3: Survey

Architectures for smart cards
J.-J. Quisquater (UCL, Louvain-la-Neuve)

Session 4: Conditional access for multimedia services

OSCAR: Open and Secure Control of Access and Rights for broadcast and switched networks
G. Maréchal (Philips, Brussels)

Equicrypt, an equitable access to multimedia services
B. Macq, J.-Y. Mertès and J.-J. Quisquater (UCL, Louvain-la-Neuve)

Session 5: Models of security

Probabilistic authentication analysis	49
J. Domingo-Ferrer (URV, Tarragona)	
An authorization model for personal databases	61
C. Radu, M. Vandenwauver, R. Govaerts and J. Vandewalle (KUL, Leuven)	

Towards testability in smart card operating system design	73
P. H. Hartel (U. of Amsterdam) and E. K. de Jong Frz (QC consultancy)	

Session 6: Electronic cash

Hardware-based off-line IC-card identification	
B. Arazi (Ben Gurion Univ.)	

A fast off-line electronic currency protocol for smart cards.....	89
Lei Tang and J. D. Tygar (CMU, Pittsburgh)	

Off-line cash transfer by smart cards	101
S. Brands (CWI, Amsterdam)	

SCALPS, Smart Card Applied to Low Payment System	119
J.-F. Dhem, J.-J. Quisquater and D. Veithen (UCL, Louvain-la-Neuve)	

Session 7: Panel

Research, progress and normalization: Is it compatible?	
Moderator: B. Arazi	

Session 8: Servers for smart cards

A universal server for smart cards	133
P. Durant, J. Bérubé, G. Lavoie, A. Gamache, P. Arduin, M.-J. Papillon and J.-P. Fortin (UL, Québec)	

Worldwide smart card services.....	141
J.-J. Vandewalle (R2DP, Lille), P. Paradinas (RD2P/Gemplus) and A. Gamache (UL, Québec)	

A smartcard fault-tolerant authentication server	149
L. Blain and Y. Deswarte (LAAS, Toulouse)	

Session 9: Panel

From smart cards to nomadic objects	
Moderator: Vincent Cordonnier	