

Table of Contents

Invited Talk

New PKI Protocols Using Tamper Resistant Hardware.....	1
<i>Peter Landrock</i>	

Certificates

Validation Algorithms for a Secure Internet Routing PKI	17
<i>David Montana and Mark Reynolds</i>	
Instant Revocation	31
<i>Jon A. Solworth</i>	
Optimized Certificates – A New Proposal for Efficient Electronic Document Signature Validation	49
<i>Ricardo Felipe Custódio, Martín A. Gagliotti Vigil, Julianio Romani, Fernando Carlos Pereira, and Joni da Silva Fraga</i>	

Authentication

An Efficient and Provable Secure Identity-Based Identification Scheme in the Standard Model	60
<i>Ji-Jian Chin, Swee-Huay Heng, and Bok-Min Goi</i>	
Trust-Rated Authentication for Domain-Structured Distributed Systems	74
<i>Ralph Holz, Heiko Niedermayer, Peter Hauck, and Georg Carle</i>	
Levels of Assurance and Reauthentication in Federated Environments	89
<i>Manuel Sánchez, Óscar Cánovas, Gabriel López, and Antonio F. Gómez-Skarmeta</i>	

Practice

Current Status of Japanese Government PKI Systems	104
<i>Yasuo Miyakawa, Takashi Kurokawa, Akihiro Yamamura, and Yasushi Matsumoto</i>	
A Privacy-Preserving eHealth Protocol Compliant with the Belgian Healthcare System	118
<i>Bart De Decker, Mohamed Layouni, Hans Vangheluwe, and Kristof Verslype</i>	

Signatures

Fast Point Decompression for Standard Elliptic Curves	134
<i>Billy Bob Brumley and Kimmo U. Järvinen</i>	
An Efficient Strong Key-Insulated Signature Scheme and Its Application	150
<i>Go Ohtake, Goichiro Hanaoka, and Kazuto Ogawa</i>	
Efficient Generic Forward-Secure Signatures and Proxy Signatures	166
<i>Basel Alomair, Krishna Sampigethaya, and Radha Poovendran</i>	

Analysis

Fault Attacks on Public Key Elements: Application to DLP-Based Schemes	182
<i>Chong Hee Kim, Philippe Bulens, Christophe Petit, and Jean-Jacques Quisquater</i>	
Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks	196
<i>Kristian Gjøsteen</i>	

Networks

An Open Mobile Identity Tool: An Architecture for Mobile Identity Management	207
<i>Konstantin Hyppönen</i>	
PEACHES and Peers	223
<i>Massimiliano Pala and Sean W. Smith</i>	
Author Index	239