

Table of Contents

Introduction to the Belgian EID Card	1
<i>D. De Cock, K. Wouters, and B. Preneel</i>	
The EuroPKI Experience	14
<i>A. Lioy, M. Marian, N. Moltchanova, and M. Pala</i>	
CERVANTES – A Certificate Validation Test-Bed	28
<i>J.L. Muñoz, J. Forné, O. Esparza, and M. Soriano</i>	
Flexible and Scalable Public Key Security for SSH	43
<i>Y. Ali and S. Smith</i>	
What Is Possible with Identity Based Cryptography for PKIs and What Still Must Be Improved	57
<i>B. Libert and J.-J. Quisquater</i>	
Identity-Based Cryptography in Public Key Management	71
<i>D.H. Yum and P.J. Lee</i>	
Pre-production Methods of a Response to Certificates with the Common Status – Design and Theoretical Evaluation	85
<i>S. Koga, J.-C. Ryou, and K. Sakurai</i>	
Filling the Gap between Requirements Engineering and Public Key/Trust Management Infrastructures	98
<i>P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone</i>	
A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications	112
<i>T. Straub and H. Baier</i>	
Using LDAP Directories for Management of PKI Processes	126
<i>V. Karatsiolis, M. Lippert, and A. Wiesmaier</i>	
Recursive Certificate Structures for X.509 Systems	135
<i>S. Russell</i>	
A Probabilistic Model for Evaluating the Operational Cost of PKI-based Financial Transactions	149
<i>A. Platis, C. Lambrinoudakis, and A. Leros</i>	

A Practical Approach of X.509 Attribute Certificate Framework as Support to Obtain Privilege Delegation.....	160
<i>J.A. Montenegro and F. Moya</i>	
TACAR: a Simple and Fast Way for Building Trust among PKIs	173
<i>D.R. Lopez, C. Malagon, and L. Florio</i>	
On the Synergy Between Certificate Verification Trees and PayTree-like Micropayments	180
<i>J. Domingo-Ferrer</i>	
A Socially Inspired Reputation Model	191
<i>N. Mezzetti</i>	
Using EMV Cards for Single Sign-On	205
<i>A. Pashalidis and C.J. Mitchell</i>	
Distributing Security-Mediated PKI	218
<i>G. Vanrenen and S. Smith</i>	
Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography	232
<i>C. Zouridaki, B.L. Mark, K. Gaj, and R.K. Thomas</i>	
ÆTHER: an Authorization Management Architecture for Ubiquitous Computing.....	246
<i>P.G. Argyroudis and D. O'Mahony</i>	
Trustworthy Accounting for Wireless LAN Sharing Communities.....	260
<i>E.C. Efstathiou and G.C. Polyzos</i>	
Mobile Qualified Electronic Signatures and Certification on Demand	274
<i>H. Rossnagel</i>	
Performance Evaluation of Certificate Based Authentication in Integrated Emerging 3G and Wi-Fi Networks.....	287
<i>G. Kambourakis, A. Rouskas, and D. Gritzalis</i>	
A Credential Conversion Service for SAML-based Scenarios	297
<i>Ó. Cánovas, G. López, and A.F. Gómez-Skarmeta</i>	
A New Design of Privilege Management Infrastructure with Binding Signature Semantics.....	306
<i>K. Bicakci and N. Baykal</i>	
How to Qualify Electronic Signatures and Time Stamps	314
<i>D. Hühnlein</i>	

An Efficient Revocation Scheme for Stateless Receivers.....	322
<i>Y.H. Hwang, C.H. Kim, and P.J. Lee</i>	
On the Use of Weber Polynomials in Elliptic Curve Cryptography	335
<i>E. Konstantinou, Y.C. Stamatou, and C. Zaroliagis</i>	
Threshold Password-Based Authentication Using Bilinear Pairings	350
<i>S. Lee, K. Han, S.-k. Kang, K. Kim, and S.R. Ine</i>	
An Efficient Group Key Management Scheme for Secure Multicast with Multimedia Applications	364
<i>C.N. Zhang and Z. Li</i>	
Author Index	379

Public Key Infrastructure

First European PKI Workshop: Research and

Applications, EuroPKI 2004, Samos Island, Greece, June

25-26, 2004, Proceedings

Katsikas, S.K.; Gritzalis, S. (Eds.)

2004, XIV, 386 p., Softcover

ISBN: 978-3-540-22216-3