Over the past years, Public Key Infrastructure (PKI) technology has evolved and moved from the research laboratories to the mainstream, in which many organizations are now leveraging it as part of their core infrastructure system for providing and building security in their businesses. Understanding the challenges and requirements of PKI related operations through the sharing of case studies are critical to supporting the continued research and development of PKI technologies and related systems and applications to further progress and innovate for enhancing future development and evolution of PKI in the enterprises. This publication includes topics such as: PKI Operation & Case Study, Non-repudiation, Authorization & Access Control, Authentication & Time-Stamping, Certificate Validation & Revocation, and Cryptographic Applications.
Contents:

PKI Operation & Case Study
- PKI Challenges: An Industry Analysis/ Geraint Price
- Directory Based Registration in Public Key Infrastructures/ M. Lippert, E. Karatsiolis, A. Wiesmaier, and J. Buchmann
- On Automatically Detecting Malicious Imposter Emails/ Erhan J. Kartaltepe and Shouhuai Xu

Non-repudiation
- Generic Fair Non-Repudiation Protocols with Transparent Off-line TTP/ Guilin Wang
- No Author-Based Selective Receipt in Certified Email with Tight Trust Requirements/ Nicolas Gonzalez-Deleito

Authorization & Access Control
- A Generic Protocol for Controlling Access to Mobile Services/ Shuhong Wang, Yingjiu Li, Bo Zhu, and Nan Hu
- Use of XACML Policies for a Network Access Control Service/ Gabriel Lopez, Oscar Canovas, and Antonio F. Gomez-Skarmeta
- A Delegation Logic Based Authorization Mechanism for Virtual Organizations/ Chunhua Gu, Xueqin Zhang, and Guoxin Song

Authentication & Time-Stamping
- An Efficient and Flexible Scheme to Support Biometric-Based and Role-Based Access Control/ Deholo Nali, Carlisle Adams, and Ali Miri
- A Study on a Framework of Online Biometric Authentication with Verification of Personal Repository/ Yoshifumi Ueshige and Kouichi Sakurai
- On Universal Composable Security of Time-Stamping Protocols/ Toshihiko Matsuo and Shin’ichiro Matsuo

Certificate Validation & Revocation
- Augmented CRL Scheme/ A. Lakshminarayanan
- Speeding up X.509 Certificate Path Validation/ Shingo Hane, Takahiro Fujiyoshi, Yoko Hashimoto, Tadashi Kaji, Kondo Katsuhiko, and Satoru Tezuka
- A Lightweight Delegated Privileges Revocation Scheme Based on Coding/ M. Francisco Hinarejos and Jordi Forne

Cryptographic Applications
- Hiding Data Sources in P2P Networks/ Marek Klonowski, Mirosław Kutylowski, and Bartłomiej Rozanski
- Efficient Broadcast from Trapdoor Functions/ Yi Mu, Willy Susilo, and Xinyi Huang
- A Generic Scheme for Zero-Knowledge Sets/ Rui Xue, Dawn Song, Zhenfeng Zhang, and Dengguo Feng

-ORDER ONLINE AT WWW.IOSPRESS.NL OR FILL IN THIS FORM-
Select the title of your choice and click on order online.

Order form:

IOS Press
Nieuwe Hemweg 6B
1013 BG Amsterdam
The Netherlands
Fax: +31 20 687 0039

IOS Press/Lavis Marketing
73 Lime Walk
Headington, Oxford
OX3 7AD, UK
Fax: +44 18 657 50079

IOS Press, Inc.
4502 Rachel Manor Drive
Fairfax, VA 22032 USA
Tel. +1 703 323 5600
Fax: +1 703 323 3668

If you would like to order one or more copies of the above, please fill in this order form and send it back to:
IOS Press, Promotion Department, Nieuwe Hemweg 6B, 1013 BG, Amsterdam, The Netherlands.

O I would like to order .... copies of Applied Public Key Infrastructure
(US$108 / €90 / £62)

O Please bill me

O Please charge my credit card
O Amer. Express
O Euro/Master
O Visa
Exp. Date
Security code

Card no.

Name:
Address:
City/Zipcode:

Country:

Fax:

E-mail:

Date:

Signature:

Visit our website for more information or online ordering:
www.iospress.nl