Public Key Infrastructure Second European Pki Workshop Research And Applications Europki 2005 Canterbury Uk June 30 July 1 2005 Revised Selected Papers Lecture Notes In Computer Science

"This book compiles estimable research on the global trend toward the rapidly increasing use of information technology in the public sector, discussing such issues as e-government and e-commerce; project management and information technology evaluation; system design and data processing; security and protection; and privacy, access, and ethics of public information technology"--Provided by publisher.

This book constitutes the refereed proceedings of the Second International Workshop on Practice and Theory in Public Key Cryptography, PKC'99, held in Kamakura, Japan in March 1999. The 25 revised full papers presented were carefully reviewed and selected from a total of 61 submissions. The volume reports most recent research results on all relevant aspects in public key cryptography. Among the topics covered are digital signatures, anonymous finger printing, message authentication, digital payment, key escrow, RSA systems, hash functions, decision oracles, random numbers, finite field computations, pay-per-view-systems, and electronic commerce.

IT policies are set in place to streamline the preparation and development of information communication technologies in a particular setting. IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications is a comprehensive collection of research on the features of modern organizations in order to advance the understanding of IT standards. This is an essential reference source for researchers, scholars, policymakers, and IT managers as well as organizations interested in carrying out research in IT policies.

This book constitutes the thoroughly refereed post-conference proceedings of the 8th European Workshop on Public Key Infrastructures, Services and Applications, EuroPKI 2011, held in Leuven, Belgium in September 2011 - co-located with the 16th European Symposium on Research in Computer Security, ESORICS 2011. The 10 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 27 submissions. The papers are organized in topical sections on authentication mechanisms, privacy preserving techniques, PKI and secure applications.

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited

The two-volume set LNCS 9614 and 9615 constitutes the refereed proceedings of the 19th IACR International Conference on the Practice and Theory in Public-Key Cryptography, PKC 2016, held in Taipei, Taiwan, in March 2016. The 34 revised papers presented were carefully reviewed and selected from 143 submissions. They are organized in topical sections named: CCA security, functional encryption, identity-based encryption, signatures, cryptanalysis, leakage-resilient and circularly secure encryption, protocols, and primitives.

This book constitutes the refereed proceedings of the 5th European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2008, held in Trondheim, Norway, in June 2008. The 15 revised full papers presented together with 1 invited paper were carefully reviewed and selected from 37 submissions. Ranging from theoretical and foundational topics to applications and regulatory issues in various contexts, the papers focus on all research and practice aspects of PKI and show ways how to construct effective, practical, secure and low cost means for assuring authenticity and validity of public keys used in large-scale networked services.

Although Internet governance deals with the core of the digital world, governance cannot be handled with the digital-binary logic of the true or false, or good or bad. Instead, the subject demands many subtleties and shades of meaning and perception, requiring an analogue approach, covering a continuum of options and compromises. The aim of the book An Introduction to Internet Governance, by Dr Jovan Kurbalija, is to provide a comprehensive overview of the main issues and actors in the field through a practical framework for analysis, discussion, and resolution of significant issues. Written in a clear and accessible way, supplemented with figures and illustrations, it focuses on the technical, security, legal, economic, development, sociocultural, and human rights aspects of Internet governance. The text and approaches presented in the book have been used by DiploFoundation and many universities as a basis from training courses and capacity development programmes on Internet governance.

These proceedings represent the work of contributors to the 19th European Conference on Cyber Warfare and Security (ECCWS 2020), supported by University of Chester, UK on 25-26 June 2020. The Conference Co-chairs are Dr Thaddeus Eze and Dr Lee Speakman, both from University of Chester and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited. ECCWS is a well-established event on the academic research calendar and now in its 19th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

This book constitutes the thoroughly refereed post-proceedings of the 2nd European Public Key Infrastructure Workshop: Research and Applications, EuroPKI 2005, held in Canterbury, UK, in June/July 2005. The 18 revised full papers presented were carefully reviewed and selected from 43 submissions. The papers are organized in topical sections on authorization, risks/attacks to PKI systems, interoperability between systems, evaluating a CA, ID ring based signatures, new protocols, practical implementations, and long term archiving.

The 2004 Information Security Conference was the seventh in a series that started with the Information Security Workshop in 1997. A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in di?erent aspects of information security. This trend c-
tinuedintheprogramofthisyear’sconference.Theprogramcommitteereceived 106 submissions, from which 36 were selected for presentation. Each submission was reviewed by at least three experts in the relevant research area. We would
liketothankalltheauthorsfortakingtheirtimetopreparethesubmissions,and
wehopethatthosewhosepapersweredeclinedwillbeableto?ndanalternative forum for their work. We were fortunate to have an energetic team of experts who took on the task of the program committee. Their names may be found overleaf, and we thank them warmly for their time and e?orts. This team was helped by an even larger number of external reviewers who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete. We would also like to thank the advisory committee for their advice and s-
port.TheexcellentlocalarrangementswerehandledbyDirkBalfanzandJessica Staddon. We made use of the electronic submission and reviewing software s- plied by COSIC at the Katholieke Universiteit Leuven. Both the software and the ISC 2004 website were run on a server at UNC Charlotte, and were perfectly maintained by Seung-Hyun Im. We also appreciate assistance from Lawrence Teo in editing the proceedings.

Electronic commerce applications all allow the transfer of electronic data from one point to another. Open EDI--a particular application of electronic commerce--also permits commercial transactions to take place in a fully automated and highly organised trading environment. This volume focuses on open EDI and its relationship with law. When confronted with technology, the typical reaction of the law is to support interpretations and amendments of existing statutes so that old laws can accommodate the change. Open EDI, however, does not fit within this traditional regulatory method. Open EDI permits ad hoc open electronic transactions irrespective of geographical border and jurisdictions among trading partners with no prior trade relationship. By doing so, open EDI limits the possibility of using up-front interchange agreements to address the legal problems of the interchange. It therefore requires the use of legal instruments supported by information technology to overcome legal problems. Openness in an electronic environment has the potential to initiate an unobserved change in law. Possible regulations should address users' need to act in such a trading environment without the inhibition of basic legal concerns. Open EDI and Law in Europe concludes that the challenge of open EDI necessitates working toward a new legal framework based on international law and supported by information technology. This volume will assist lawyers and laypersons concerned with the practical and theoretical aspects of the legal issues of the application of open EDI by pointing out subtle issues in the application of law in this area and by provoking thought regarding possible solutions.

Public Key InfrastructureSecond European PKI Workshop: Research and Applications, EuroPKI 2005, Canterbury, UK, June 30- July 1, 2005, Revised Selected PapersSpringer Science & Business Media

This book presents the most interesting talks given at ISSE 2009 – the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Economics of Security and Identity Management - Security Services and Large Scale Public Applications - Privacy and Data Protection and Awareness Raising - Standards and Technical Solutions - Secure Software, Trust and Assurance Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2009.

This book constitutes the refereed proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, held in Melbourne, Victoria, Australia, in January 2000. The 31 revised full papers presented were carefully reviewed and selected from 70 submissions. Among the topics addressed are cryptographic protocols, digital signature schemes, elliptic curve cryptography, discrete logarithm, authentication, encryption protocols, key recovery, time stamping, shared cryptography, certification, zero-knowledge proofs, auction protocols, and mobile communications security.

Here are the refereed proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography, PKC 2006, held in New York City in April 2006. The 34 revised full papers presented are organized in topical sections on cryptanalysis and protocol weaknesses, distributed crypto-computing, encryption methods, cryptographic hash and applications, number theory algorithms, pairing-based cryptography, cryptosystems design and analysis, signature and identification, authentication and key establishment, multi-party computation, and PKI techniques.

Thisbookcontainsthepostproceedingsofthe6thEuropeanWorkshoponPublic Key Services, Applications and Infrastructures, which was held at the CNR Research Area in Pisa, Italy, in September 2009. The EuroPKI workshop series focuses on all research and practice aspects of public key infrastructures, services and applications, and welcomes original research papers and excellent survey contributions from academia, government, and industry. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); Turin, Italy, (2006); Palma de Mallorca, Spain, (2007); and Trondheim, Norway (2008). From the original focus on public key infrastructures, EuroPKI interests - panded to include advanced cryptographic techniques, applications and (more generally) services. The Workshops brings together researchersfrom the cryp- graphiccommunity as well as fromthe applied security community, as witnessed by the interesting program. Indeed, this volume holds 18 refereed papers and the presentation paper by the invited speaker, Alexander Dent. In response to the EuroPKI 2009 call for papers, a total of 40 submissions were received. All submissions underwent a thorough blind review by at least three ProgramCommittee members, resulting in careful selection and revision of the accepted papers. After the conference, the papers were revised and improved by the authors before inclusion in this volume.

This unique text deals with the most important legal areas for e-commerce related business in most of the member states in Europe as well as the USA. Topics that are dealt with include: contract law, consumer protection, intellectual property law, unfair competition, antitrust law, liability of providers, money transactions, privacy and data protection.

The second generation Digital Tachograph system, called Smart Tachograph, has been introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council. Annex 1C of the Commission Implementing Regulation (EU) 2016/799 lays down the technical requirements for the construction, testing, installation, operation and repair of Smart Tachographs and their components. Appendix 11 (Common Security Mechanisms) of Annex 1C specifies the security mechanisms ensuring - Mutual authentication between different components of the tachograph system. - Confidentiality, integrity, authenticity and/or non-repudiation of data transferred between different components of the tachograph system or downloaded to external storage media. Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realise this for the second-generation tachograph system. A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic systems rely on master keys that have to be delivered to the relevant actors. An infrastructure consisting of three layers has been set up. At the European level, the European Root Certification Authority (ERCA) is responsible for the generation and management of root public-private key pairs, with the respective certificates, and symmetric master keys. The ERCA issues certificates to Member State Certification Authorities (MSCAs) and distributes symmetric master keys to the MSCAs. The MSCAs are responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment. Next to the production keys and certificates, the ERCA also issues test certificates and distributes test symmetric master keys to MSCAs to be used for Interoperability Testing purposes, Using these test keys and certificates, MSCAs can sign and distribute certificates, symmetric keys and encrypted data for motion sensors to be installed in Smart Tachograph equipment for interoperability testing purposes. This document forms the Certificate Policy (CP) for the PKI at the ERCA level. It lays down the policy at ERCA level for key generation, key management and certificate signing for the Smart Tachograph system. For the ERCA to issue certificates to an MSCA or to distribute symmetric keys to an MSCA, the MSCA shall comply with requirements also laid down in this document. This document follows the framework for CPs described in RFC 3647. The Symmetric Key Infrastructure policy has been added to this document, preserving the lay-out of RFC 3647. How the ERCA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the ERCA Certification Practice Statement (CPS).The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119.

This book constitutes the refereed proceedings of the First European Public Key Infrastructure Workshop: Research and Applications, EuroPKI 2004, held on Samos Island, Greece in June 2004. The 25 revised full papers and 5 revised short papers presented were carefully reviewed and selected from 73 submissions. The papers address all current issues in PKI, ranging from theoretical and foundational topics to applications and regulatory issues in various contexts.

This book constitutes the thoroughly refereed joint post-proceedings of the three International Workshops on Grid Middleware, CoreGrid 2006, the UNICORE Summit 2006, and the Workshop on Petascale Computational Biology and Bioinformatics, held in Dresden, Germany, in August/September 2006, in conjunction with Euro-Par 2006, the 12th International Conference on Parallel Computing.

The Cryptographers' Track (CT-RSA) is a research conference within the RSA conference, the largest, regularly staged computer security event. CT-RSA 2004 was the fourth year of the Cryptographers' Track, and it is now an established venue for presenting practical research results related to cryptography and data security. The conference received 77 submissions, and the program committee sel- ted 28 of these for presentation. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryp- graphy. Each paper was reviewed by at least three program committee members. Extended abstracts of the revised versions of these papers are in these proc- dings. The program also included two invited lectures by Dan Boneh and Silvio Micali. I am extremely grateful to the program committee members for their en- mous investment of time and e?ort in the di?cult and delicate process of review and selection. Many of them attended the program committee meeting during the Crypto 2003 conference at the University of California, Santa Barbara.

This book contains the proceedings of the Second European Conference on Computer Network Defence, which took place in December 2006. The conference focused on the protection of computer networks and attracted participants from national and international organisations. The papers collected in this book include contributions from leading figures in the field and are a valuable source of reference for both researcher and practitioner.

This book contains the proceedings of the 2nd EuroPKI Workshop — EuroPKI 2005, held at the University of Kent in the city of Canterbury, UK, 30 June–1 July 2005. The workshop was informal and lively, and the university setting encouragedactive exchangesbetween the speakersand the audience. TheworkshopprogramcomprisedakeynotespeechfromDr.CarlisleAdams, followedby18refereedpapers,withaworkshopdinnerinandguidedtouraround the historic Dover Castle. Dr. Adams is well known for his contributions to the CAST family of s- metric encryption algorithms, to international standards from the IETF, ISO, and OASIS, authorship of over 30 refereed journals and conference papers, and co-authorship of Understanding PKI: Concepts, Standards, and Deployment Considerations (Addison-Wesley). Dr. Adams keynote speech was entitled 'PKI: Views from the Dispassionate "I",' in which he presented his thoughts on why PKIhas been availableas an authentication technology for many years now,but has only enjoyed large-scale success in fairly limited contexts to date. He also presented his thoughts on the possible future(s) of this technology, with emp- sis on the major factors hindering adoption and some potential directions for future research in these areas. In response to the Call for Papers, 43 workshop papers were submitted in total. All papers were blind reviewed by at least two members of the Program Committee, the majority having 3 reviewers, with a few borderline papers h- ing 4 or more reviewers; 18 papers were accepted for presentation in 8 sessions.

This volume contains the proceedings of the IFIPTM 2008, the Joint iTrust and PST Conferences on Privacy, Trust Management and Security, held in Trondheim, Norway from June 18 to June 20, 2008. IFIPTM 2008 provides a truly global platform for the reporting of research, development, policy and practice in the interdependent areas of Privacy, Security, and Trust. Following the traditions inherited from the highly successful iTrust and PST conference series, IFIPTM 2008 focuses on trust, privacy and security from multidisciplinary perspectives. The conference is an arena for discussion about re levant problems from both research and practice in the areas of academia, busi ness, and government. IFIPTM 2008 is an open IFIP conference, which only accepts contributed pa pers, so all papers in these proceedings have passed strict peer review. The pro gram of the conference features both theoretical research papers and reports of real world case studies. IFIPTM 2008 received 62 submissions. The program commit tee selected 22 papers for presentation and inclusion in the proceedings. In addi tion, the program and the proceedings include 3 demo descriptions. The highlights of IFIPTM 2008 include invited talks and tutorials by industri al and academic experts in the fields of trust management, privacy and security, including Jon Bing and Michael Steiner.

This volume focuses on the latest findings concerning financial environment research and the effects on business. Major topics addressed range from finance-driven globalization, contagion risk transmission, financial sustainability, and bank efficiency, to oil price shocks and spot prices research. Further topics include family business, business valuation, public sector development and business organization in the globalized environment. This book features selected peer-reviewed articles from the 16th EBES conference in Istanbul, where over 270 papers were presented by 478 researchers from 56 countries.

Finck examines the emergence of blockchains (and other forms of distributed ledger technologies) and the implications for regulation and governance.

This book constitutes the refereed proceedings of the 4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks, ESAS 2007, held in Cambridge, UK, in July 2007. The papers present original research on all aspects of security and privacy in wireless ad hoc and sensor networks and address current topics of network security, cryptography, and wireless networking communities.

This book presents the most interesting talks given at ISSE 2012 - the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Information Security Strategy; Enterprise and Cloud Computing Security - Security and Privacy Impact of Green Energy; Human Factors of IT Security - Solutions for Mobile Applications; Identity & Access Management - Trustworthy Infrastructures; Separation & Isolation - EU Digital Agenda; Cyber Security: Hackers & Threats Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2012. Content Information Security Strategy - Enterprise and Cloud Computing Security - Security and Privacy - Impact of Green Energy - Human Factors of IT Security - Solutions for Mobile Applications - Identity & Access Management - Trustworthy Infrastructures - Separation & Isolation - EU Digital Agenda - Cyber Security - Hackers & Threats Target Group Developers of Electronic Business Processes IT Managers IT Security Experts Researchers The Editors Norbert Pohlmann: Professor for Distributed System and Information Security at Westfälische Hochschule Gelsenkirchen Helmut Reimer: Senior Consultant, TeleTrusT Wolfgang Schneider: Senior Adviser, Fraunhofer Institute SIT

Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. Here the positions of the experts involved are very diverse: some strive for as much security as possible, others only for as much security as is necessary. The conference ISSE (Information Security Solutions Europe) is the outstanding forum for the interdisciplinary search for sustainable compromises and for the presentation of concepts which hold up in real life. This book offers the most recent papers in the area of strategies, technologies, applications and best practice.

This book constitutes the refereed proceedings of the Third European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2006, held in Torino, Italy, in June 2006. The 18 revised full papers and 4 short papers presented were carefully reviewed and selected from about 50 submissions. The papers are organized in topical sections on PKI management, authentication, cryptography, applications, and short contributions.

26th European Symposium on Computer Aided Process Engineering contains the papers presented at the 26th European Society of Computer-Aided Process Engineering (ESCAPE) Event held at Portorož Slovenia, from June 12th to June 15th, 2016. Themes discussed at the conference include Process-product Synthesis, Design and Integration, Modelling, Numerical analysis, Simulation and Optimization, Process Operations and Control and Education in CAPE/PSE. Presents findings and discussions from the 26th European Society of Computer-Aided Process Engineering (ESCAPE) Event

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.

This volume critically explores the contentions in the emerging debate surrounding new media technologies and the extent to which they are challenging traditional political and government models. Examining a range of citizen/government interactions which together form e-government in different contexts, this book assesses the potential of new media technologies to facilitate new institutional patterns for governance and participation, as experienced primarily, but not only, across Europe. Analysing a range of challenges spanning from those of a technological and conceptual nature to those of a more political and legal nature, the authors scrutinise the central policies at governmental and organisational levels and consider the following questions: Is society driving or responding to e-government and is it ready to cope with it? What implications does e-government have for the power/democracy relationship? Is the technology right for e-government? What is needed to ensure government services are delivered optimally? How is e-government perceived and is it trusted? How are the sensitive issues of identity, privacy and social inclusion dealt with? How are management and safety dealt with when one considers issues such as activism, cyberterrorism, biometrics, and new implications for international relations? This comprehensive text will be of interest to students and scholars of public policy, politics, media and communication studies, sociology, law and European studies. It will also offer insights of relevance to practitioners and policy-makers in regional, national, and transnational governance, reform and innovation.

This volume features the refereed proceedings from the 4th European Public Key Infrastructure Workshop: Theory and Practice, held in Palma de Mallorca, Spain in June 2007. Twenty-one full papers and eight short papers, contributed by experts in the field, are included. The papers address all current issues in public key infrastructure, ranging from theoretical and foundational topics to applications and regulatory issues.

The 2nd European AcrossGrids Conference (AxGrids 2004) aimed to examine the state of the art in research and technology developments in Grid Computing, and provide a forum for the presentation and exchange of views on the latest grid-related research results and future work. The conference was organized by Cross Grid, a European Union-funded project on Grid research, GRIDSTART, the EU-sponsored initiative for consolidating technical advances in grids in - rope, and the University of Cyprus. It continued on from the successful 1st European Across Grids Conference, held in Santiago de Compostela, Spain, in February 2003. AxGrids 2004 was run in conjunction with the 2nd IST Conc- tation Meeting on Grid Research, which brought together representatives from all EU-funded projects on Grid research for an exchange of experiences and ideas regarding recent developments in European grid research. The conference was hosted in Nicosia, the capital of Cyprus, and attracted- thors and attendees from all over Europe, the USA, and East Asia. The Program Committee of the conference consisted of 37 people from both academia and - dustry, and there were 13 external reviewers. Overall, AxGrids 2004 attracted 57 paper submissions (42 full papers and 15 short posters). Papers underwent a thorough review by several Program Committee members and external - viewers. After the review, the Program Chair decided to accept 26 papers (out of 42) for regular presentations, 8 papers for short presentations, and 13 - pers for poster presentations. Accepted papers underwent a second review for inclusion this postproceedings volume, published as part of Springer's Lecture Notes in Computer Science series.

This first-of-its-kind book, from expert authors actively contributing to the evolution of Bluetooth specifications, provides an overview and detailed descriptions of all the security functions and features of this standard's latest core release. After categorizing all the security issues involved in ad hoc networking, this hands-on volume shows you how to design a highly secure Bluetooth system and implement security enhancements. The book also helps you fully understand the main security risks involved with introducing Bluetooth-based communications in your organization.

Whether the reader is the biggest technology geek or simply a computer enthusiast, this integral reference tool can shed light on the terms that'll pop up daily in the communications industry. (Computer Books - Communications/Networking)