Sokratis K. Katsikas
Stefanos Gritzalis
Javier Lopez (Eds.)

LNCS 3093

Public Key Infrastructure

**First European PKI Workshop:
Research and Applications, EuroPKI 2004
Samos Island, Greece, June 2004, Proceedings**

Springer

Sokratis K. Katsikas Stefanos Gritzalis
Javier Lopez (Eds.)

Public Key Infrastructure

First European PKI Workshop:
Research and Applications, EuroPKI 2004
Samos Island, Greece, June 25-26, 2004
Proceedings

Springer

Volume Editors

Sokratis K. Katsikas
University of the Aegean
Rector's Office, Administration Building
University Hill, GR-81100 Mytilene, Greece
E-mail: ska@aegean.gr

Stefanos Gritzalis
University of the Aegean
Department of Information and Communication Systems Engineering
Laboratory of Information and Communication Systems Security
Karlovassi, GR-83200 Samos, Greece
E-mail: sgritz@aegean.gr

Javier Lopez
University of Malaga
Computer Science Department, E.T.S. Ingeniería Informática
Campus de Teatinos, Spain
E-mail: jlm@lcc.uma.es

Library of Congress Control Number: 2004107465

CR Subject Classification (1998): E.3, D.4.6, C.2.0, F.2.1, H.3, H.4, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-22216-2 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 11012214 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3093

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Lecture Notes in Computer Science

For information about Vols. 1–2986

please contact your bookseller or Springer-Verlag

Vol. 3093: S.K. Katsikas, S. Gritzalis, J. Lopez (Eds.), Public Key Infrastructure. XIII, 380 pages. 2004.

Vol. 3092: J. Eckstein, H. Baumeister (Eds.), Extreme Programming and Agile Processes in Software Engineering. XVI, 358 pages. 2004.

Vol. 3091: V. van Oostrom (Ed.), Rewriting Techniques and Applications. X, 313 pages. 2004.

Vol. 3089: M. Jakobsson, M. Yung, J. Zhou (Eds.), Applied Cryptography and Network Security. XIV, 510 pages. 2004.

Vol. 3085: S. Berardi, M. Coppo, F. Damiani (Eds.), Types for Proofs and Programs. X, 409 pages. 2004.

Vol. 3084: A. Persson, J. Stirna (Eds.), Advanced Information Systems Engineering. XIV, 596 pages. 2004.

Vol. 3083: W. Emmerich, A.L. Wolf (Eds.), Component Deployment. X, 249 pages. 2004.

Vol. 3078: S. Cotin, D.N. Metaxas (Eds.), Medical Simulation. XVI, 296 pages. 2004.

Vol. 3077: F. Roli, J. Kittler, T. Windeatt (Eds.), Multiple Classifier Systems. XII, 386 pages. 2004.

Vol. 3076: D. Buell (Ed.), Algorithmic Number Theory. XI, 451 pages. 2004.

Vol. 3074: B. Kuijpers, P. Revesz (Eds.), Constraint Databases and Applications. XII, 181 pages. 2004.

Vol. 3073: H. Chen, R. Moore, D.D. Zeng, J. Leavitt (Eds.), Intelligence and Security Informatics. XV, 536 pages. 2004.

Vol. 3070: L. Rutkowski, J. Siekmann, R. Tadeusiewicz, L.A. Zadeh (Eds.), Artificial Intelligence and Soft Computing - ICAISC 2004. XXV, 1208 pages. 2004. (Subseries LNAI).

Vol. 3068: E. André, L. Dybkj\ae r, W. Minker, P. Heisterkamp (Eds.), Affective Dialogue Systems. XII, 324 pages. 2004. (Subseries LNAI).

Vol. 3066: S. Tsumoto, R. S lowiński, J. Komorowski, J.W. Grzymala-Busse (Eds.), Rough Sets and Current Trends in Computing. XX, 853 pages. 2004. (Subseries LNAI).

Vol. 3065: A. Lomuscio, D. Nute (Eds.), Deontic Logic in Computer Science. X, 275 pages. 2004. (Subseries LNAI).

Vol. 3064: D. Bienstock, G. Nemhauser (Eds.), Integer Programming and Combinatorial Optimization. XI, 445 pages. 2004.

Vol. 3063: A. Llamosí, A. Strohmeier (Eds.), Reliable Software Technologies - Ada-Europe 2004. XIII, 333 pages. 2004.

Vol. 3062: J.L. Pfaltz, M. Nagl, B. Böhlen (Eds.), Applications of Graph Transformations with Industrial Relevance. XV, 500 pages. 2004.

Vol. 3060: A.Y. Tawfik, S.D. Goodwin (Eds.), Advances in Artificial Intelligence. XIII, 582 pages. 2004. (Subseries LNAI).

Vol. 3059: C.C. Ribeiro, S.L. Martins (Eds.), Experimental and Efficient Algorithms. X, 586 pages. 2004.

Vol. 3058: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 233 pages. 2004.

Vol. 3056: H. Dai, R. Srikant, C. Zhang (Eds.), Advances in Knowledge Discovery and Data Mining. XIX, 713 pages. 2004. (Subseries LNAI).

Vol. 3054: I. Crnkovic, J.A. Stafford, H.W. Schmidt, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 311 pages. 2004.

Vol. 3053: C. Bussler, J. Davies, D. Fensel, R. Studer (Eds.), The Semantic Web: Research and Applications. XIII, 490 pages. 2004.

Vol. 3052: W. Zimmermann, B. Thalheim (Eds.), Abstract State Machines 2004. Advances in Theory and Practice. XII, 235 pages. 2004.

Vol. 3051: R. Berghammer, B. Möller, G. Struth (Eds.), Relational and Kleene-Algebraic Methods in Computer Science. X, 279 pages. 2004.

Vol. 3050: J. Domingo-Ferrer, V. Torra (Eds.), Privacy in Statistical Databases. IX, 367 pages. 2004.

Vol. 3047: F. Oquendo, B. Warboys, R. Morrison (Eds.), Software Architecture. X, 279 pages. 2004.

Vol. 3046: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1016 pages. 2004.

Vol. 3045: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1040 pages. 2004.

Vol. 3044: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1140 pages. 2004.

Vol. 3043: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1180 pages. 2004.

Vol. 3042: N. Mitrou, K. Kontovasilis, G.N. Rouskas, I. Iliadis, L. Merakos (Eds.), NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. XXXIII, 1519 pages. 2004.

Vol. 3039: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1271 pages. 2004.

Vol. 3038: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1311 pages. 2004.

Vol. 3037: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 745 pages. 2004.

Vol. 3036: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 713 pages. 2004.

Vol. 3035: M.A. Wimmer (Ed.), Knowledge Management in Electronic Government. XII, 326 pages. 2004. (Subseries LNAI).

Vol. 3034: J. Favela, E. Menasalvas, E. Chávez (Eds.), Advances in Web Intelligence. XIII, 227 pages. 2004. (Subseries LNAI).

Vol. 3033: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVIII, 1076 pages. 2004.

Vol. 3032: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVII, 1112 pages. 2004.

Vol. 3031: A. Butz, A. Krüger, P. Olivier (Eds.), Smart Graphics. X, 165 pages. 2004.

Vol. 3030: P. Giorgini, B. Henderson-Sellers, M. Winikoff (Eds.), Agent-Oriented Information Systems. XIV, 207 pages. 2004. (Subseries LNAI).

Vol. 3029: B. Orchard, C. Yang, M. Ali (Eds.), Innovations in Applied Artificial Intelligence. XXI, 1272 pages. 2004. (Subseries LNAI).

Vol. 3028: D. Neuenschwander, Probabilistic and Statistical Methods in Cryptology. X, 158 pages. 2004.

Vol. 3027: C. Cachin, J. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT 2004. XI, 628 pages. 2004.

Vol. 3026: C. Ramamoorthy, R. Lee, K.W. Lee (Eds.), Software Engineering Research and Applications. XV, 377 pages. 2004.

Vol. 3025: G.A. Vouros, T. Panayiotopoulos (Eds.), Methods and Applications of Artificial Intelligence. XV, 546 pages. 2004. (Subseries LNAI).

Vol. 3024: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 621 pages. 2004.

Vol. 3023: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 611 pages. 2004.

Vol. 3022: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 621 pages. 2004.

Vol. 3021: T. Pajdla, J. Matas (Eds.), Computer Vision - ECCV 2004. XXVIII, 633 pages. 2004.

Vol. 3019: R. Wyrzykowski, J.J. Dongarra, M. Paprzycki, J. Wasniewski (Eds.), Parallel Processing and Applied Mathematics. XIX, 1174 pages. 2004.

Vol. 3016: C. Lengauer, D. Batory, C. Consel, M. Odersky (Eds.), Domain-Specific Program Generation. XII, 325 pages. 2004.

Vol. 3015: C. Barakat, I. Pratt (Eds.), Passive and Active Network Measurement. XI, 300 pages. 2004.

Vol. 3014: F. van der Linden (Ed.), Software Product-Family Engineering. IX, 486 pages. 2004.

Vol. 3012: K. Kurumatani, S.-H. Chen, A. Ohuchi (Eds.), Multi-Agnets for Mass User Support. X, 217 pages. 2004. (Subseries LNAI).

Vol. 3011: J.-C. Régin, M. Rueher (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. XI, 415 pages. 2004.

Vol. 3010: K.R. Apt, F. Fages, F. Rossi, P. Szeredi, J. Váncza (Eds.), Recent Advances in Constraints. VIII, 285 pages. 2004. (Subseries LNAI).

Vol. 3009: F. Bomarius, H. Iida (Eds.), Product Focused Software Process Improvement. XIV, 584 pages. 2004.

Vol. 3008: S. Heuel, Uncertain Projective Geometry. XVII, 205 pages. 2004.

Vol. 3007: J.X. Yu, X. Lin, H. Lu, Y. Zhang (Eds.), Advanced Web Technologies and Applications. XXII, 936 pages. 2004.

Vol. 3006: M. Matsui, R. Zuccherato (Eds.), Selected Areas in Cryptography. XI, 361 pages. 2004.

Vol. 3005: G.R. Raidl, S. Cagnoni, J. Branke, D.W. Corne, R. Drechsler, Y. Jin, C.G. Johnson, P. Machado, E. Marchiori, F. Rothlauf, G.D. Smith, G. Squillero (Eds.), Applications of Evolutionary Computing. XVII, 562 pages. 2004.

Vol. 3004: J. Gottlieb, G.R. Raidl (Eds.), Evolutionary Computation in Combinatorial Optimization. X, 241 pages. 2004.

Vol. 3003: M. Keijzer, U.-M. O'Reilly, S.M. Lucas, E. Costa, T. Soule (Eds.), Genetic Programming. XI, 410 pages. 2004.

Vol. 3002: D.L. Hicks (Ed.), Metainformatics. X, 213 pages. 2004.

Vol. 3001: A. Ferscha, F. Mattern (Eds.), Pervasive Computing. XVII, 358 pages. 2004.

Vol. 2999: E.A. Boiten, J. Derrick, G. Smith (Eds.), Integrated Formal Methods. XI, 541 pages. 2004.

Vol. 2998: Y. Kameyama, P.J. Stuckey (Eds.), Functional and Logic Programming. X, 307 pages. 2004.

Vol. 2997: S. McDonald, J. Tait (Eds.), Advances in Information Retrieval. XIII, 427 pages. 2004.

Vol. 2996: V. Diekert, M. Habib (Eds.), STACS 2004. XVI, 658 pages. 2004.

Vol. 2995: C. Jensen, S. Poslad, T. Dimitrakos (Eds.), Trust Management. XIII, 377 pages. 2004.

Vol. 2994: E. Rahm (Ed.), Data Integration in the Life Sciences. X, 221 pages. 2004. (Subseries LNBI).

Vol. 2993: R. Alur, G.J. Pappas (Eds.), Hybrid Systems: Computation and Control. XII, 674 pages. 2004.

Vol. 2992: E. Bertino, S. Christodoulakis, D. Plexousakis, V. Christophides, M. Koubarakis, K. Böhm, E. Ferrari (Eds.), Advances in Database Technology - EDBT 2004. XVIII, 877 pages. 2004.

Vol. 2991: R. Alt, A. Frommer, R.B. Kearfott, W. Luther (Eds.), Numerical Software with Result Verification. X, 315 pages. 2004.

Vol. 2990: J. Leite, A. Omicini, L. Sterling, P. Torroni (Eds.), Declarative Agent Languages and Technologies. XII, 281 pages. 2004. (Subseries LNAI).

Vol. 2989: S. Graf, L. Mounier (Eds.), Model Checking Software. X, 309 pages. 2004.

Vol. 2988: K. Jensen, A. Podelski (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XIV, 608 pages. 2004.

Vol. 2987: I. Walukiewicz (Ed.), Foundations of Software Science and Computation Structures. XIII, 529 pages. 2004.

Preface

There is no doubt that the Internet is affecting every aspect of our lives; the most significant changes are occurring in private and public sector organizations that are transforming their conventional operating models to Internet-based service models, known as eBusiness, eCommerce and eGovernment. Companies, institutions and organizations, irrespective of their size, are nowadays utilizing the Internet for communicating with their customers, suppliers and partners; for facilitating the interconnection of their employees and branches; for connecting to their back-end data systems and for performing commercial transactions. In such an environment, where almost every organization relies heavily on information and communications technologies, new dependencies and risks arise. *Public Key Infrastructure (PKI)* is probably one of the most important items in the arsenal of security measures that can be brought to bear against the aforementioned growing risks and threats.

PKI research has been active for more than 26 years. In 1978 R.L. Rivest, A. Shamir and L. Adleman published what is now commonly called the RSA cryptosystem (*Communications of the ACM,* Vol.21, No.2, pp.120–128, 1978), one of the most significant discoveries in the history of cryptography. Since the mathematical foundation of RSA rests on the intractability of factoring large composite integers, in the same year, R. Merkle demonstrated that certain computational puzzles could also be used in constructing public key cryptography (*Communications of the ACM,* Vol.21, No.4, pp.194–299, 1978).

As the years passed by, several countries started developing their PKI. Inevitably, several practical problems were identified. Although adhering to international standards, such as ITU, ISO, IETF and PKCS, different PKI systems (national and/or international) could not connect to one another. Subsequently, a number of organizations were formed to promote and support the interoperability of different PKIs between certain countries. Indicative examples of such organizations today include the *PKI Forum,* the *EESSI – European Electronic Signature Standardization Initiative* and the *Asia PKI Forum.*

To foster and stimulate these discussions in a research environment, the *International Workshops for Asian PKI (IWAP)* and the *US PKI Research Workshops* have been held annually since 2001 (IWAP 2001 in Korea, IWAP 2002 in Taiwan, IWAP 2004 in Japan) and since 2002 (the annual US PKI Research Workshops, hosted by the NIST) respectively. Their goal is to provide a framework for both theoreticians and practitioners to share their experience and research outcomes concerning good practices in applying PKI and related supporting technologies, together with prudent assessment and comparison of the technologies.

The first *European PKI Workshop: Research and Applications (EuroPKI 2004)* initiated a series of corresponding workshop activities in Europe. The EuroPKI 2004 workshop was held on 25–26 June 2004, on Samos Island, Greece, and was hosted by the University of the Aegean, Department of Information and Communication Systems Engineering, Laboratory of Information and Communication Systems Security (*Info-Sec-Lab*, www.icsd.aegean.gr/Info-Sec-Lab).

In response to the EuroPKI 2004 call for papers, 73 papers were submitted, whose authors came from 25 countries. Each paper was reviewed by three members of the Program Committee, on the basis of the significance, novelty, technical quality and PKI relevance of the work reported therein. At the end of the reviewing process, only 25 papers were selected for presentation, whose authors came from 13 countries, resulting in an acceptance rate of 34%. This volume contains these papers as well as 5 additional short papers.

We would like to thank all the members of the Program Committee, as well as the external reviewers, for their constructive and insightful comments during the review process. Moreover, we would like to express our gratitude to the members of the Organizing Committee for their continuous and valuable support. We also wish to express our thanks to Alfred Hofmann and his colleagues from Springer-Verlag, for their co-operation and their excellent work during the publication process. Finally, we would like to thank all the people who submitted their papers to the workshop, including those whose submissions were not selected for publication, and all the delegates from around the world who attended the first *European PKI Workshop*. Without their support the workshop would not have been possible.

June 2004

Sokratis K. Katsikas
Stefanos Gritzalis
Javier Lopez

EuroPKI'2004 Workshop Committee

General Chairman

Sokratis K. Katsikas	University of the Aegean, Greece

Program Committee Co-Chairmen

Stefanos Gritzalis	University of the Aegean, Greece
Javier Lopez	University of Malaga, Spain

International Program Committee

Carlisle Adams	University of Ottawa, Canada
Giampaolo Bella	University of Catania, Italy
Ahto Buldas	Tallinn Technical University, Estonia
Mike Burmester	Florida State University, USA
Luke O'Connor	IBM, Switzerland
Sabrina De Capitani di Vimercati	University of Milan, Italy
Vassilios Chryssikopoulos	Ionian University, Greece
Ed Dawson	Queensland University of Technology, Australia
Yves Deswarte	LAAS-CNRS, France
Stephen Farrell	Trinity College Dublin, Ireland
Simon Foley	University College Corke, Ireland
Jordi Forne	Polytechnic University of Catalonia, Spain
Steven Furnell	University of Plymouth, UK
Dieter Gollmann	TU Hamburg-Harburg, Germany
Antonio Gomez-Skarmeta	University of Murcia, Spain
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Hideki Imai	University of Tokio, Japan
Sushil Jajodia	George Mason University, USA
Kwangjo Kim	Information and Communications University, Korea
Spyros Kokolakis	University of the Aegean, Greece
Constantinos Lambrinoudakis	University of the Aegean, Greece
Dimitris Lekkas	University of the Aegean, Greece
Peter Lipp	Technical University of Graz, Austria
Jose A. Mañas	Polytechnic University of Madrid, Spain
Catherine Meadows	NRL, USA

Chris Mitchell	RHBNC, University of London, UK
Refik Molva	Eurécom, France
Eiji Okamoto	University of Tsukuba, Japan
Rolf Oppliger	eSecurity, Switzerland
George Pangalos	Aristotelean University of Thessaloniki, Greece
Ahmed Patel	University College Dublin, Ireland
Guenther Pernul	University of Regensburg, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Gerald Quirchmayr	University of South Australia, Australia
Jean-Jacques Quisquater	UCL, Belgium
Peter Ryan	University of Newcastle, UK
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Sean Smith	Dartmouth College, USA
Diomidis Spinellis	Athens University of Economics and Business, Greece
Julien P. Stern	Cryptolog, France
Michael Szydlo	RSA Security Inc., USA
Moti Yung	Columbia University, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

George Aggelis	University of the Aegean, Greece
Carlos Aguilar	LAAS-CNRS, France
Walid Bagga	Institut Eurecom, France
Thodoris Balopoulos	University of the Aegean, Greece
Phil Brooke	University of Plymouth, UK
Jeremy Bryans	University of Newcastle-upon-Tyne, UK
Oscar Canovas	University of Murcia, Spain
Shiping Chen	George Mason University, USA
Lazaros Gymnopoulos	University of the Aegean, Greece
DongGuk Han	Kyushu University, Japan
John Iliadis	University of the Aegean, Greece
Kenji Imamoto	Kyushu University, Japan
George Kambourakis	University of the Aegean, Greece
Satoshi Koga	Kyushu University, Japan
Gregorio Martinez	University of Murcia, Spain
Gabriel López Millán	University of Murcia, Spain
Lilian Mitrou	University of the Aegean, Greece
Björn Muschall	University of Regensburg, Germany
Melek Onen	Institut Eurecom, France

Akira Otsuka	Information Technology Promotion Agency, Japan
Thea Peacock	University of Newcastle-upon-Tyne, UK
Josep Pegueroles	Technical University of Catalonia, Spain
Agapios Platis	University of the Aegean, Greece
Fabien Pouget	Institut Eurecom, France
Torsten Priebe	University of Regensburg, Germany
Thomas Quillinan	University College Corke, Ireland
Junji Shikata	Yokohama National University, Japan
BHan Shin	Tokyo University, Japan
Seong Han Shin	Tokyo University, Japan
Vasileios Vlachos	Athens University of Economics and Business, Greece
Chao Yao	George Mason University, USA
Alec Yasinsac	Florida State University, USA
Rui Zhang	Tokyo University, Japan
Sencun Zhu	George Mason University, USA

Table of Contents

Introduction to the Belgian EID Card
BELPIC

Danny De Cock*, Karel Wouters*, and Bart Preneel

Katholieke Universiteit Leuven,
Department of Electrical Engineering–ESAT SCD/COSIC
Kasteelpark Arenberg 10, B-3001 Heverlee-Leuven, Belgium
http://www.esat.kuleuven.ac.be/cosic
{decockd,kwouters,preneel}@esat.kuleuven.ac.be

Abstract. This article gives a brief introduction to the Belgian EID card project commonly referred to as "Belpic." This introduction includes an overview of the history of the project, details on the visual and cryptographic aspects of the EID cards, a discussion of the different sub-CAs involved, together with the card issuing process.

Key words: Electronic IDentity card (EID), nation-wide Public-Key Infrastructure (PKI), legally significant certificates, authentication certificates, qualified certificates, Certificate Revocation Lists (CRL).

1 Introduction and Scope

Belgium is planning to be the first European country that distributes Electronic IDentity (EID) cards with digital signature technology to *all* its citizens. One of the main incentives to introduce the EID card is to increase the openness of the administration towards the citizen: on the short term, citizens will have access to their own population file to check who was in dialogue with their file during the last months, to trace in what stage is the answer on their request to get a building permit, etc. These are only a few possible uses of the card. Within a few years from now these use cases will have evolved and extended in a variety of new ways, both in the communication channel between the government and its citizens, and between organizations and their customers.

Benefits. All commercial, not-for-profit and governmental players such as banking, insurance, health care, etc. can benefit from the EID card to improve their quality of service without having to implement and deploy their own public-key infrastructure (PKI). They will be able to offer secure remote enrollment, strong entity authentication and digital signatures without the large and expensive overhead of PKI and smart card deployment. Moreover, all entities will

* The author was partially supported by the GOA project MEFISTO 2000/6 of the Flemish Government

S.K. Katsikas et al. (Eds.): EuroPKI 2004, LNCS 3093, pp. 1–13, 2004.

have the guarantee from the Belgian government that the citizen/customer has been identified correctly and that the card and its protocols have been evaluated for security. This technology will also significantly decrease the risk for identity theft.

In the short term, the EID card will increase the confidence level of identification information used in the public and commercial sector through a more accurate collection of a citizen's identity data. This will result in an increased use of secure identification and authentication technology in multiple applications, both for governmental and other environments. For many individual applications the issuance of such a card and the establishment of a PKI architecture was not economically feasible, but the EID card allows to reduce this cost.

By January 1st, 2004 all EU member states were required to implement e-invoicing in their national legislation [11]. One condition is that the authenticity of the origin and the integrity of the content is guaranteed, for instance by relying on advanced electronic signatures. It is clear that the current EID card can fulfill these conditions.

Costs and limitations. Today, the citizen pays 12 EUR when he collects his/her EID card, which is about twice as much as for a non-electronic identity card. From the government side, a large investment in infrastructure and management is required in the move to the electronic version.

The current EID card only authenticates the identity of the sender, not his role within the organization or his authorization to perform a certain action (such as sending an invoice) in the first place. This requires application-dependent solutions. Moreover, it has been decided not to support private-key decryption for the pilot phase, in part because of the problem of key recovery for back-up purposes.

One can anticipate that the financial sector (such as the credit card industry, retail payments) will keep issuing its own cards and managing its own PKI architecture. There are several reasons for this: first, they have invested heavily in past years in this environment. To implement a worldwide deployment (e.g., EMV technology in the credit cards); second, they prefer to control their own environment both in terms of technology, risk management and marketing (logos on the card). Finally, multi-application smart cards with secure separation between the applications have not yet reached the required maturity level. One can however expect that the EID card will be used as a bootstrap mechanism for retail e-banking.

The current EID certificates include the name and RRN number (National Register number) of the holder; this is an 11-digit number consisting of the date of birth (dd/mm/yy format), 3 digits reflecting a sequence counter and 2 check digits. This number should be considered as sensitive personal data. Unfortunately, the design of the RRN number makes it rather trivial to guess. The RRN number is used by the government (and by some health care organizations) as a link to the identity of the card holder, because it is the key used as input to many databases containing information about the citizen. The inclusion of the name and RRN number of the citizen in the certificate attached to every transaction