LNCS 4043

Andrea S. Atzeni
Antonio Lioy (Eds.)

Public Key Infrastructure

Third European PKI Workshop: Theory and Practice, EuroPKI 2006 Turin, Italy, June 2006, Proceedings

Springer

Andrea S. Atzeni   Antonio Lioy (Eds.)

Public Key Infrastructure

Third European PKI Workshop:
Theory and Practice, EuroPKI 2006
Turin, Italy, June 19-20, 2006
Proceedings

Springer

Volume Editors

Andrea S. Atzeni
Antonio Lioy
Politecnico di Torino
Dip. di Automatica ed Informatica
Corso Duca degli Abruzzi, 24, 10129 Torino, Italy
E-mail: {shocked,lioy}@polito.it

Library of Congress Control Number: 2006927052

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-35151-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35151-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11774716 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4043

Preface

Today, PKIs have come of age and they support the security of several large networked systems, such as company-wide document management systems, e-government applications and secure VPN. However, despite this success, the field has not yet reached its full scientific maturity and there is still room for research in this area. For example, open issues exist in the efficient management of large PKI (especially with respect to certificate validation), better performance could be attained by improved cryptographic techniques and innovative applications are continuously proposed.

To discuss progress in the PKI field, the European PKI workshop series was established in 2004, following similar initiatives in Asia and the USA. The first two events of this series took place on the Island of Samos, Greece (EuroPKI 2004), and in Canterbury, UK (EuroPKI 2005).

This book contains the proceedings of the Third European PKI Workshop (EuroPKI 2006), held at the Politecnico di Torino, Italy, on June 19-20, 2006. In response to the Call for Papers, about 50 submissions were received. All submissions were reviewed by at least two reviewers (external or members of the Program Committee) and most of them got three reviews. At the end of this process, 22 papers were selected, 18 in their full form and 4 as short papers. These papers led to a lively workshop, with a good mixture between theory and application, continuing the success of the previous workshops in the series.

I would like to thank the authors for their papers, the Program Committee and external reviewers for their efforts during the review process, and finally all the workshop participants, without whom the workshop would have not been successful.

June 2006 Antonio Lioy

Organization

EuroPKI 2006 was organized by the TORSEC Computer and Network Security Group (http://security.polito.it) at the Dipartimento di Automatica ed Informatica of the Politecnico di Torino, in cooperation with the Istituto Superiore Mario Boella.

Program Chairman

Antonio Lioy

Organizing Chairman

Andrea S. Atzeni

Program Committee

A. Buldas, University of Tartu (Estonia)
D. Chadwick, University of Kent (UK)
S. Farrell, Trinity College Dublin (Ireland)
S. Furnell, University of Plymouth (UK)
D. Gollmann, Hamburg University of Technology (Germany)
S. Gritzalis, University of the Aegean (Greece)
Y. Karabulut, SAP AG (Germany)
S. Katsikas, University of the Aegean (Greece)
S. Kent, BBN (USA)
K. Kim, Information and Communications Univ. (Korea)
A. Lioy, Politecnico di Torino (Italy)
J. Lopez, Universidad de Malaga (Spain)
F. Martinelli, IIT-CNR (Italy)
F. Maino, Cisco (USA)
D. Mazzocchi, ISMB (Italy)
C. Mitchell, Royal Holloway (UK)
W. Schneider, Fraunhofer SIT (Germany)
A. Vaccarelli, IIT-CNR (Italy)

External Reviewers

A. Atzeni, Politecnico di Torino (Italy)
M. Aime, Politecnico di Torino (Italy)

D. Berbecaru, Politecnico di Torino (Italy)
A. Dent, Royal Holloway (UK)
J. Haller, SAP AG (Germany)
F. Kerschbaum, SAP AG (Germany)
J. Iliadis, University of the Aegean (Greece)
D. Lekkas, University of the Aegean (Greece)
C. Lambrinoudakis, University of the Aegean (Greece)
G. Morgari, Telsy (Italy)
M. Pala, Politecnico di Torino (Italy)
K. Paterson, Royal Holloway (UK)
G. Ramunno, Politecnico di Torino (Italy)
G. Sburlati, IIT-CNR (Italy)

Sponsor

Istituto Superiore Mario Boella, Torino, Italy

Lecture Notes in Computer Science

For information about Vols. 1–3929

please contact your bookseller or Springer

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Applications in Management. XI, 395 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.

Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.

Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).

Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.

Vol. 4024: S. Donatelli, P. S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.

Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).

Vol. 4013: L. Lamontagne, M. Marchand (Eds.), Advances in Artificial Intelligence. XIII, 564 pages. 2006. (Sublibrary LNAI).

Vol. 4011: Y. Sure, J. Domingue (Eds.), The Semantic Web: Research and Applications. XIX, 726 pages. 2006.

Vol. 4010: S. Dunne, B. Stoddart (Eds.), Unifying Theories of Programming. VIII, 257 pages. 2006.

Vol. 4007: C. Àlvarez, M. Serna (Eds.), Experimental Algorithms. XI, 329 pages. 2006.

Vol. 4006: L.M. Pinho, M. González Harbour (Eds.), Reliable Software Technologies – Ada-Europe 2006. XII, 241 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 4001: E. Dubois, K. Pohl (Eds.), Advanced Information Systems Engineering. XVI, 560 pages. 2006.

Vol. 3999: C. Kop, G. Fliedl, H.C. Mayr, E. Métais (Eds.), Natural Language Processing and Information Systems. XIII, 227 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), Algorithms and Complexity. XII, 394 pages. 2006.

Vol. 3997: W. Grieskamp, C. Weise (Eds.), Formal Approaches to Software Testing. XII, 219 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part IV. XXXV, 1096 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part III. XXXVI, 1136 pages. 2006.

Vol. 3992: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part II. XXXV, 1122 pages. 2006.

Vol. 3991: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part I. LXXXI, 1096 pages. 2006.

Vol. 3990: J. C. Beck, B.M. Smith (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 301 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao, Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), Location- and Context-Awareness. X, 289 pages. 2006.

Vol. 3986: K. Stølen, W.H. Winsborough, F. Martinelli, F. Massacci (Eds.), Trust Management. XIV, 474 pages. 2006.

Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part V. XXV, 1045 pages. 2006.

Vol. 3983: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part IV. XXVI, 1191 pages. 2006.

Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part III. XXV, 1243 pages. 2006.

Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part II. XXVI, 1255 pages. 2006.

Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part I. LXXV, 1199 pages. 2006.

Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, M. Kölsch, A. Galata, B. Kisačanin (Eds.), Computer Vision in Human-Computer Interaction. XII, 121 pages. 2006.

Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 179 pages. 2006. (Sublibrary LNAI).

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), Networking 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. XXVI, 1276 pages. 2006.

Vol. 3975: S. Mehrotra, D.D. Zeng, H. Chen, B.M. Thuraisingham, F.-Y. Wang (Eds.), Intelligence and Security Informatics. XXII, 772 pages. 2006.

Vol. 3973: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part III. XXIX, 1402 pages. 2006.

Vol. 3972: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part II. XXVII, 1444 pages. 2006.

Vol. 3971: J. Wang, Z. Yi, J.M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part I. LXVII, 1442 pages. 2006.

Vol. 3970: T. Braun, G. Carle, S. Fahmy, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 350 pages. 2006.

Vol. 3968: K.P. Fishkin, B. Schiele, P. Nixon, A. Quigley (Eds.), Pervasive Computing. XV, 402 pages. 2006.

Vol. 3967: D. Grigoriev, J. Harrison, E.A. Hirsch (Eds.), Computer Science – Theory and Applications. XVI, 684 pages. 2006.

Vol. 3966: Q. Wang, D. Pfahl, D.M. Raffo, P. Wernick (Eds.), Software Process Change. XIV, 356 pages. 2006.

Vol. 3965: M. Bernardo, A. Cimatti (Eds.), Formal Methods for Hardware Verification. VII, 243 pages. 2006.

Vol. 3964: M. Ü. Uyar, A.Y. Duale, M.A. Fecko (Eds.), Testing of Communicating Systems. XI, 373 pages. 2006.

Vol. 3963: O. Dikenelli, M.-P. Gleizes, A. Ricci (Eds.), Engineering Societies in the Agents World VI. XII, 303 pages. 2006. (Sublibrary LNAI).

Vol. 3962: W. IJsselsteijn, Y. de Kort, C. Midden, B. Eggen, E. van den Hoven (Eds.), Persuasive Technology. XII, 216 pages. 2006.

Vol. 3960: R. Vieira, P. Quaresma, M.d.G.V. Nunes, N.J. Mamede, C. Oliveira, M.C. Dias (Eds.), Computational Processing of the Portuguese Language. XII, 274 pages. 2006. (Sublibrary LNAI).

Vol. 3959: J.-Y. Cai, S. B. Cooper, A. Li (Eds.), Theory and Applications of Models of Computation. XV, 794 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3955: G. Antoniou, G. Potamias, C. Spyropoulos, D. Plexousakis (Eds.), Advances in Artificial Intelligence. XVII, 611 pages. 2006. (Sublibrary LNAI).

Vol. 3954: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part IV. XVII, 613 pages. 2006.

Vol. 3953: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part III. XVII, 649 pages. 2006.

Vol. 3952: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part II. XVII, 661 pages. 2006.

Vol. 3951: A. Leonardis, H. Bischof, A. Pinz (Eds.), Computer Vision – ECCV 2006, Part I. XXXV, 639 pages. 2006.

Vol. 3950: J.P. Müller, F. Zambonelli (Eds.), Agent-Oriented Software Engineering VI. XVI, 249 pages. 2006.

Vol. 3948: H.I Christensen, H.-H. Nagel (Eds.), Cognitive Vision Systems. VIII, 367 pages. 2006.

Vol. 3947: Y.-C. Chung, J.E. Moreira (Eds.), Advances in Grid and Pervasive Computing. XXI, 667 pages. 2006.

Vol. 3946: T.R. Roth-Berghofer, S. Schulz, D.B. Leake (Eds.), Modeling and Retrieval of Context. XI, 149 pages. 2006. (Sublibrary LNAI).

Vol. 3945: M. Hagiya, P. Wadler (Eds.), Functional and Logic Programming. X, 295 pages. 2006.

Vol. 3944: J. Quiñonero-Candela, I. Dagan, B. Magnini, F. d'Alché-Buc (Eds.), Machine Learning Challenges. XIII, 462 pages. 2006. (Sublibrary LNAI).

Vol. 3943: N. Guelfi, A. Savidis (Eds.), Rapid Integration of Software Engineering Techniques. X, 289 pages. 2006.

Vol. 3942: Z. Pan, R. Aylett, H. Diener, X. Jin, S. Göbel, L. Li (Eds.), Technologies for E-Learning and Digital Entertainment. XXV, 1396 pages. 2006.

Vol. 3941: S.W. Gilroy, M.D. Harrison (Eds.), Interactive Systems. XI, 267 pages. 2006.

Vol. 3940: C. Saunders, M. Grobelnik, S. Gunn, J. Shawe-Taylor (Eds.), Subspace, Latent Structure and Feature Selection. X, 209 pages. 2006.

Vol. 3939: C. Priami, L. Cardelli, S. Emmott (Eds.), Transactions on Computational Systems Biology IV. VII, 141 pages. 2006. (Sublibrary LNBI).

Vol. 3936: M. Lalmas, A. MacFarlane, S. Rüger, A. Tombros, T. Tsikrika, A. Yavlinsky (Eds.), Advances in Information Retrieval. XIX, 584 pages. 2006.

Vol. 3935: D. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A. C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3933: F. Bonchi, J.-F. Boulicaut (Eds.), Knowledge Discovery in Inductive Databases. VIII, 251 pages. 2006.

Vol. 3931: B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri (Eds.), Neural Nets. XIII, 370 pages. 2006.

Vol. 3930: D.S. Yeung, Z.-Q. Liu, X.-Z. Wang, H. Yan (Eds.), Advances in Machine Learning and Cybernetics. XXI, 1110 pages. 2006. (Sublibrary LNAI).

Author Index

Table of Contents

PKI Management

Authentication I

Cryptography

Applications

Authentication II

Short Contributions

Use of a Validation Authority to Provide Risk Management for the PKI Relying Party

Jon Ølnes[1] and Leif Buene[2]

[1] DNV Research, Veritasveien 1, N-1322 Høvik, Norway
[2] DNV Certification, Veritasveien 1, N-1322 Høvik, Norway
{jon.olnes, leif.buene}@dnv.com

Abstract. Interoperability between PKIs (Public Key Infrastructure) is a major issue in several electronic commerce scenarios. A Relying Party (RP), in particular in an international setting, should not unduly put restrictions on selection of Certificate Authorities (CA) by its counterparts. Rather, the RP should be able to accept certificates issued by any relevant CA. Such acceptance implies not only the ability to validate certificates, but also an assessment of the risk related to acceptance of a certificate for the purpose at hand. We analyse common PKI trust models with respect to risk management, and argue that an independent, trusted Validation Authority (VA) may be a better approach for this task. A VA as suggested by this paper will also remove the need for complicated certificate path processing.

1 Introduction

Public key cryptography used with a PKI (Public Key Infrastructure) carries the promise of authentication, electronic signatures and encryption based on sharing of only non-secret information (public keys, names and other information in certificates[1]). The same information (the certificate) may be shared with all counterparts, to replace separate, shared secrets.

The counterpart (RP for Relying Party – relying on certificates) must be able to validate the certificate (with respect to validity period, revocation status, authenticity, and integrity) and interpret its content. In addition, the RP must decide if the quality of the certificate is sufficient for the purpose at hand, and whether or not to accept the issuer of the certificate (the CA – Certification Authority). The latter decisions should be based on evaluation of the risk to the RP.

While the quality of a certificate (chiefly determined by the CA's certificate policy) in most cases is the primary risk element, other aspects of the CA itself, such as

[1] Another term is "electronic ID". A PKI-based electronic ID usually consists of two or three certificates and corresponding key pairs, separating out the encryption (key negotiation) function and possibly also the electronic signature (non-repudiation) function to separate key pairs/certificates. To a user, this separation is normally not visible. This paper uses the term "certificate", to be interpreted as covering the electronic ID term where appropriate.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 1 – 15, 2006.

nationality, financial status, and reputation may be important. Note also that the policy represents a claimed quality level, and assessment of compliance may be important. An RP will typically also be very interested in the liability taken on by the CA in case of errors, and the possibility for claiming liability if needed.

It is clear that, in particular in an international setting, an RP may need to accept certificates from a large number of CAs. Present approaches to interoperability are trust lists (trusted CAs and their public keys) and formation of trust structures (hierarchy, cross-certification, and bridge-CA) among CAs. We argue that all these approaches have shortcomings with respect to aiding the RP's risk management decisions. Trust structures imply the need to discover and validate potentially complex trust paths through the structures, a major concern in present PKI implementations.

This paper recommends a different approach, where interoperability is offered by means of a trusted Validation Authority (VA), serving as an independent trust anchor for the RP. The VA serves as a clearinghouse between CAs and RPs, and by trusting the VA the RP is able to trust all CAs that the VA answers for.

The model is based on policies and explicit, signed agreements. An overall validation policy for the VA's services is defined, and additionally RPs may define individual policies to tailor services to their needs. The RP has one agreement with the VA, and the VA on the other hand has agreements with the CAs, preferably in a model where one VA-CA agreement covers all RPs that the VA handles. Thus, all actors (including the CAs) obtain a clear risk picture. The VA handles all CAs individually, and as an added value the need for cumbersome certificate path discovery and validation procedures is removed. The RP obtains a one-stop shopping service for acceptance of certificates – one point of trust, one agreement, one bill, one liable actor.

In this trust model, it is important that the VA is neutral with respect to CAs, i.e. the VA service should be offered by an independent actor. In particular, this applies to judgments about quality and other aspects of CAs and their services.

In the following, we clarify DNV's position in 2, describe requirements in 3, take a critical look at existing approaches in 4, describe the independent VA in 5, present elements for certificate validation policies in 6, and conclude in 7.

2 DNV's Position and Role

DNV (Det Norske Veritas, http://www.dnv.com) is an independent foundation offering classification and certification services from offices in more than 100 countries. The maritime sector and the oil and gas industry are the main markets. DNV is also among the world's leading certification bodies for management systems (ISO 9000, ISO 14000, BS 7799 and others), delivering services to all market sectors.

DNV seeks to extend its existing position as a supplier of trusted third party services to digital communication and service provisioning. The first version of a VA service along the lines described in this paper will be offered to pilot customers 3Q 2006. This paper does not describe this pilot service but rather the research leading to the decision to launch the pilot service.

3 The PKI Interoperability Challenge and Scaling

In general, the certificate holder and the RP can be independent entities, who may independently select the CAs to obtain certificates from; then:

- A certificate holder should be able to use the same certificate towards all relevant RPs, regardless of the CA(s) used by the RP itself.
- An RP (e.g. a service provider in an international market) should be able to use and validate certificates from all relevant certificate holders, regardless of the CA of the certificate holder.
- When a digitally signed document is created, the parties involved may be able to identify the relevant CAs. However, the document may need to be verified later by another actor, who may not have any relationship to any of these CAs.

The set of relevant counterparts, and thus the set of relevant CAs, may be limited by criteria such as nationality or business/application area. However, unlimited interoperability may be viewed as the ultimate goal, likened to the ability to make phone calls internationally.

The challenge is primarily on the RP, which is the actor that faces the complexity of a large number of CAs. An RP must not only validate certificates but also assess the risk related to accepting a certificate for a given purpose. This paper suggests using the risk elements: quality of certificate (mainly derived from certificate policy), assessment of quality (e.g. compliance with policy), liability and possibilities to claim liability, and other aspects of the CA and its services (such as nationality). This is further discussed in 6. An uncertain risk situation may be unacceptable to the RP.

PKIs as society infrastructures are being deployed in probably most developed countries for national electronic IDs. Deployment is either based on CAs run by public authorities or on services obtained from the commercial market. Society infrastructures are almost exclusively national, although some international co-ordination takes place. Notably, the EU Directive on electronic signatures [12] defines the concepts of qualified signature/certificate as means to achieve legal harmonisation across the EU in this area. Even in countries with (plans for) public authority CAs, the usual situation is several (2–15 is typical for European countries) public, commercial CAs competing in a national market. PKI interoperability thus may be a challenge even at a national level, and interoperability at an international level is a severe challenge. Some commercial CAs, e.g. Verisign, compete in an international market.

Other PKI deployments add to the scale of the interoperability challenge. Some corporate (business internal) PKIs aim at acceptance of certificates even outside of the corporation. Community infrastructures are under establishment, some even internationally like the SAFE initiative [27] for the pharmaceutical industry. The banking and aerospace industries may be mentioned as other particularly active arenas. The educational sector is very active in the PKI area, and initiatives like the EuroPKI [22] expand the scope outside of the academic sector and internationally.

Thus, the interoperability challenge is necessarily on the agenda. One example is the IDABC (Interoperable Delivery of European E-government Services to Public Administrations, Businesses and Citizens) programme's statement on electronic public procurement [7], related to creation of an internal market[2] in the EU: "The interoperability problems detected [for qualified electronic signatures] despite the existence of standards, and the absence of a mature European market for this type of signatures pose a real and possibly persistent obstacle to cross-border e-procurement." Other examples can be found, notably also from internationally oriented businesses.

4 Present Approaches to PKI Interoperability, Risk Management

4.1 Trust Models and Certificate Paths

Present methods for PKI interoperability are lists of trusted CAs (see 4.5) and creation of trust structures among CAs by issuance of certificates to the CAs themselves; by a peer-CA, a bridge-CA, or a CA at a higher level of a hierarchy. The idea is that an RP should be able to discover and validate a certificate path from a directly trusted CA (typically the root-CA of a hierarchy) to any CA (may be previously "unknown") that is a member of the same trust structure. In this, trust is regarded as a transitive property. The number of CAs directly trusted by an RP can be reduced; however the trust decision must always be derived from a CA accepted as a "trust anchor".

In general, certificate path discovery may be a very difficult task [29], and sufficient support is lacking in many PKI implementations. Certificate path validation may be very resource demanding due to the need for repeated certificate processing. Caching of previously validated trust paths can mitigate this problem. Certificate path validation, possibly also path discovery, may be performed by a validation service (delegated path validation/discovery [30]). Note that the trust model suggested by this paper (see 5.1) eliminates certificate path processing.

In the context of this paper, "trust" not only means the ability to find a trusted copy of a CA's public key but also support for risk management by quality, assessment of quality, and liability issues (the "other aspects" element left out). Below, we examine different trust models with respect to these properties. Note that one may argue that certificate chains increase risk since there is always a >0 probability of failure for each link in the chain.

4.2 Peer-CA Cross-Certification

Peer-CA cross-certification is a mechanism where two CAs mutually (the usual situation, although one-way cross-certification is also possible) issue certificates to one another. With respect to quality, cross-certification with policy mapping means that the two CAs' services are regarded as equal. The complexity involved in the policy mapping depends on the differences in the policies. There are a few common frameworks [6] [8] [9] for structuring of policies. Mapping between the frameworks is not too complicated, and most CAs adhere to one of the frameworks. Still, the real content of policies may differ quite a lot. Without policy mapping, cross-certification may give no indication on quality of the other CA.

Cross-certification is typically carried out in a carefully scrutinized process involving assessment of the peer-CA's claimed quality. As a result, a CA may be willing to

[2] Coined as "the SEEM" (Single European Electronic Market) in EU terms.