NISTIR 7313
ISBN 1-886843-39-2

5th Annual PKI R&D Workshop
"Making PKI Easy to Use"
Proceedings

William T. Polk
Nelson E. Hastings
Kent Seamons

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NISTIR 7313
ISBN 1-886843-39-2

5th Annual PKI R&D Workshop
"Making PKI Easy to Use"
Proceedings

William T. Polk
Nelson E. Hastings
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Kent Seamons
Brigham Young University

July 2006

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary
TECHNOLOGY ADMINISTRATION
Robert Cresanti, Under Secretary of Commerce for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

Foreward

NIST hosted the fifth annual Public Key Infrastructure (PKI) R&D Workshop on April 4-6, 2006. The two and a half day event brought together PKI experts from academia, industry, and government to explore the current state of public key technology and emerging trust mechanisms, share lessons learned, and discuss complementary topics such as usability. The workshop also served as a forum to review continuing progress in focus areas from previous workshops. In addition to the seven refereed papers, this proceedings captures the essence of the workshop activities including the keynote address, four invited talks, five panels, the work-in-progress session and, new to the workshop this year, an informal rump session.

This workshop began with a variation on a familiar theme: usability. Angela Sasse presented the keynote, “Has Jonny Learnt to Encrypt By Now?”, revisiting Alma Whitten’s keynote from the 2003 workshop. Sasse’s approach emphasizes “value-based design”: by understanding the users’ goals, and designing around them, we can build a more usable system. Features and complexities not essential to the user experience should be hidden by simplifying systems and hiding complexity. Usability was also addressed in a paper session on “Easy-to-Use Deployment Architectures” and panels on digital signatures and browser security interfaces.

Improving the security of infrastructure and applications was another recurring theme throughout the workshop. A presentation on trust infrastructures and DNSSEC by Allison Mankin was given on the first day of the workshop. Although attacking DNS is straightforward, there are few incentives for attackers so DNS poisoning is relatively rare. The low threat level may be one reason that DNSSEC deployment has been slow. A panel on Domain Keys Identified Mail (DKIM), which leverages the DNS for key distribution, was held on the second day of the workshop. DKIM would seem to provide the incentive for attacking the DNS, so perhaps DNSSEC deployment will become a more urgent requirement. Phillip Hallam-Baker’s presentation on the DKIM panel, “Achieving Email Security Luxury” proposed leveraging DKIM, XKMS, and the PKIX logotype extension to create a comprehensive and compelling solution for securing applications and the infrastructure.

Another theme of the workshop was the convergence of PKI and other technologies. Jeffrey Altman’s presentation highlighted progress in the convergence of PKI and Kerberos. A decade’s efforts have produced PK-INIT, PK-CROSS, and PK-APP, forming a comprehensive suite of standards. PK-INIT and PK-APP allow users to leverage PKI certificates to obtain Kerberos credentials, and vice versa. PK-CROSS supports the establishment of Kerberos cross realm relationships with PKI credentials. The “Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy” presentation described the integration of the Grid PKIs, Security Assertion Markup Language (SAML), Kerberos, and one time passwords to support authorization decisions for Grid computing.

Identifying and resolving revocation issues continues to be a topic of critical interest. This year’s workshop featured two presentations at very different levels of abstraction. Kelvin Yiu’s invited talk focused on challenges that had to be faced and compromises required to make revocation usable for consumers in the forthcoming Vista operating system. Santosh Chokhani explored some of the more arcane nuances of the X.509

standard, and their implications for real PKI deployments. A less than cautious approach to CA key rollover or PKI architecture design can introduce circularities in trust paths when validating CRLs or OCSP responses.

The first two days of the workshop also included the ever-popular Works In Progress session. This session allowed presenters to obtain early feedback on ongoing work or projects that are in the early conceptual stages. Major WIP presentations addressed interoperability results for the Suite B cipher suites, progress in the Global Grid, and experiences with securing the DNS. In the rump session, brief presentations questioned old paradigms (e.g., are offline CAs really more secure?) and proposed novel applications of current technology (such as mobile phones as secure containers).

The workshop closed with a half day devoted to PKI deployment issues. The panel on "PKI in Higher Education" had an international flavor, featuring a presentation on the Australian CAUDIT PKI Federation. This was followed by a snapshot of U.S. government PKI deployment activities in the "Federal PKI Update" panel. The workshop ended with a look at leading edge deployment activities in the "Bridge to Bridge Interoperations" panel. Bridge-to-bridge cross certification will create policy and technology challenges, however the panel concluded that these challenges are not insurmountable.

The 150 attendees represented a cross-section of the global PKI community, with presenters from the USA, United Kingdom, Britain, Israel, Australia, Norway, Sweden, Germany and Canada. Due to the success of this event, a sixth workshop is planned for Spring 2007.

William T. Polk and Nelson E. Hastings
National Institute of Standards and Technology
Gaithersburg, MD USA

2006 PKI R&D Workshop
Making PKI Easy to Use

Gaithersburg, Maryland USA

April 4-6, 2006

http://middleware.internet2.edu/pki06/

(Pre-proceedings were distributed at the workshop)

WORKSHOP SUMMARY 1

Provided by Ben Chinowsky, Internet2

REFERRED PAPERS

How Trust Had a Hole Blown In It. The Case of X.509 Name Constraints 13

David Chadwick — *University of Kent, England*

Navigating Revocation through Eternal Loops and Land Mines 31

Santosh Chokhani — *Orion Security Solutions, Inc.*
Carl Wallace — *Orion Security Solutions, Inc.*

Simplifying Public Key Credential Management through Online Certificate Authorities and PAM 46

Stephen Chan — *NERSC/Lawrence Berkeley National Lab*
Matthew Andrews — *NERSC/Lawrence Berkeley National Lab*

Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy 54

Tom Barton — *University of Chicago*
Jim Basney — *NCSA/University of Illinois*
Tim Freeman — *University of Chicago*
Tom Scavo — *NCSA/University of Illinois*
Frank Siebenlist — *University of Chicago & MCSD, Argonne National Lab*
Von Welch — *NCSA/University of Illinois*
Rachana Ananthakrishnan — *MCSD/Argonne National Lab*
Bill Baker — *NCSA/University of Illinois*
Monte Goode — *Lawrence Berkeley National Lab*
Kate Keahey — *University of Chicago & MCSD/Argonne National Lab*

PKI Interoperability by an Independent, Trusted Validation Authority 68

Jon Ølnes — *DNV Research; Norway*

Achieving Email Security Usability 79

Phillip Hallam-Baker — *VeriSign Inc.*

CAUDIT PKI Federation - A Higher Education Sector Wide Approach **92**

Rodney McDuff — *The University of Queensland*
Viviani Paz — *Australian Computer Emergency Response Team*

LIST OF ACRONYMS **105**

Organizers

General Chair: Ken Klingenstein, University of Colorado
Program Chair: Kent Seamons, Brigham Young University
Steering Committee Chair: Neal McBurnett, Internet2
Local Arrangements Chair: Nelson Hastings, NIST
Scribe: Ben Chinowsky, Internet2

Program Committee

Kent Seamons, *Brigham Young Univ.* (chair)
Peter Alterman, *National Institutes of Health*
Stefan Brands*, Credentica and McGill Univ.*
Bill Burr, *NIST*
David Chadwick*, University of Kent*
Yassir Elley, *Forum Systems*
Carl Ellison, *Microsoft*
Stephen Farrell, *Trinity College Dublin*
Richard Guida, *Johnson & Johnson*
Jason Holt, *Brigham Young Univ.*
Russ Housley, *Vigil Security, LLC*
Ken Klingenstein, *Internet2*
Neal McBurnett, *Internet2*
Clifford Neuman, *USC-ISI*
Eric Norman, *University of Wisconsin*
Tim Polk, *NIST*
Ravi Sandhu, *GMU and TriCipher*
Krishna Sankar, *Cisco Systems*
Frank Siebenlist, *Argonne Nat'l Laboratory*
Sean Smith, *Dartmouth College*
Von Welch, *NCSA*
Stephen Whitlock*, Boeing*
Michael Wiener, *Cryptographic Clarity*
William Winsborough, *Univ. of Texas at San Antonio*

Archival Sites

PKI 2006:	http://middleware.internet2.edu/pki06
PKI 2005:	http://middleware.internet2.edu/pki05
PKI 2004:	http://middleware.internet2.edu/pki04
PKI 2003:	http://middleware.internet2.edu/pki03
PKI 2002:	http://www.cs.dartmouth.edu/~pki02

This page has been left intentionally blank.