

5th Annual PKI R&D Workshop

April 4-6, 2006 • NIST • Gaithersburg, MD

Sponsored by:
National Institute of Standards and Technology
National Institutes of Health
and Internet2
In cooperation with OASIS

This workshop considers the full range of public key technology used for security decisions and supporting functionalities, including authentication, authorization, identity (syndication, federation, and aggregation), and trust. This year, the workshop has a particular interest in novel approaches to simplifying the use and management of X.509 digital certificates, both within and across enterprises. This workshop has three goals:

1. Explore the current state of public key technology and emerging trust mechanisms in different domains including web services; grid technologies; encryption functionality; authentication systems et al., in academia, government and the private sector.
2. Share & discuss lessons learned and scenarios from vendors and practitioners on current deployments.
3. Provide a forum for leading security researchers to explore the issues relevant to the PKI space in areas of security management, identity, trust, policy, authentication, authorization and encryption (e.g., supporting privacy requirements).

REGISTRATION

The registration fee of **\$125 per person** includes workshop materials, coffee breaks, lunches, and a dinner. An agenda will be available in late December at <http://middleware.internet2.edu/pki06/>

Teresa Vicente
NIST
Phone: (301) 975-3883
Fax: (301) 948-2067
email: teresa.vicente@nist.gov

There will be no on-site registration. Please pre-register by **March 17, 2006** either electronically at www.nist.gov/conference or by contacting Teresa Vicente.

ACCOMMODATIONS

A block of rooms has been reserved at the Gaithersburg Hilton, **(301) 977-8900**, at a special rate of **\$109**, single or double, plus 12% tax. Reservations must be received by **March 17, 2006**.

CALL FOR PAPERS

We solicit papers, case studies, panel proposals, and participation from researchers, systems architects, vendor engineers, and users. Submitted works should address one or more critical areas of inquiry. Topics include (but are not limited to):

- Federated versus Non-Federated trust models
- Standards related to PKI and security decision systems, such as X.509, SPKI/SDSI, PGP, XKMS, XACML, XRML, XML signatures and SAML
- Cryptographic and alternative methods for supporting security decisions, including the characterization and encoding of data
- Intersection of assertion-based systems and PKI
- Human-Computer Interaction (HCI) advances that improve usability of PKI for users and administrators
- Privacy protection and implications
- Use of PKI in emerging technologies (i.e., sensor networks)
- Scalability of security systems
- Security of the components of PKI systems
- Security infrastructures for constrained environments

- Improved human factor designs for security-related interfaces including authorization and policy management, naming, use of multiple private keys, and selective disclosure
- New paradigms in PKI architectures
- Reports of real-world experience with the use and deployment of PKI, including the use of digital certificates with major off-the-shelf application programs, how best to integrate such usage into legacy systems, and future research directions

Deadlines for conference paper and panel submissions are:

Papers and Proposals Due:

October 14, 2005

Authors Notified:

December 2, 2005

Final Materials Due:

February 3, 2006

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11

inches). Paper submissions must not exceed 15 pages (single space, two column format with 1" margins using a 10 pt or larger font) and have no header or footer text (e.g., no page numbers). Proposals for panels should be no longer than five pages and include possible panelists and an indication of which panelists have confirmed participation.

Please submit the following information to pkichairs@internet2.edu:

- Name, affiliation, email, phone, postal address for the primary contact author
- First name, last name, and affiliation of each co-author
- The finished paper in PDF format as an attachment.

All submissions will be acknowledged. Submissions of papers must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conferences or journals.

Accepted papers will be published in a proceedings of the workshop.

PROGRAM COMMITTEE

Kent Seamons, *Brigham Young University (chair)*
Peter Alterman, *National Institutes of Health*
Stefan Brands, *Credentica and McGill University*
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 University*
Russ Housley, *Vigil Security, LLC*
Ken Klingenstein, *Internet2*
Neal McBurnett, *Internet2*
Clifford Neuman, *University of Southern California*
Eric Norman, *University of Wisconsin*
Tim Polk, *NIST*

Ravi Sandhu, *George Mason University and TriCipher*
Krishna Sankar, *Cisco Systems*
Frank Siebenlist, *Argonne National Laboratory*
Sean Smith, *Dartmouth College*
Von Welch, *NCSA*
Stephen Whitlock, *Boeing*
Michael Wiener, *Cryptographic Clarity*
William Winsborough, *University of Texas at San Antonio*

General Chair:
Ken Klingenstein
Internet2
kjk@internet2.edu

Program Chair:
Kent Seamons
Brigham Young University
seamons@cs.byu.edu

Steering Committee Chair:
Neal McBurnett
Internet2
neal@bcn.boulder.co.us

Local Arrangements Chair:
Nelson Hastings
NIST
nelson.hastings@nist.gov