

# 6<sup>th</sup> Annual PKI R&D Workshop

April 17-19, 2007 • NIST • Gaithersburg, MD

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

This workshop considers the full range of public key technology used for security decisions and supporting functionalities, including authentication, authorization, identity management, federation, and trust. This year's focus is striking the proper balance to permit users to complete tasks requiring security easily while exposing the appropriate security details through all layers of software. 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, etc., in academia, research, government, and industry.
2. Share and discuss lessons learned and scenarios encountered from vendors and practitioners from current deployments.
3. Provide a forum for leading security researchers to explore the issues relevant to PKI in relation to applications, usability, security management, identity, trust, policy, authentication, authorization and encryption (e.g., supporting privacy requirements).

## CALL FOR PAPERS

We solicit papers, case studies, panel proposals, and participation from researchers, systems architects, vendor engineers, and users. Suggested topics include but are not limited to:

- Reports of real-world experience with the use and deployment of applications that leverage PKI, how best to integrate such usage into legacy systems, and future research directions
- 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
- Identity management (Shibboleth, Liberty, Higgins, InfoCard, etc.)
- Cryptographic and alternative methods for supporting security decisions, including the characterization and encoding of data
- Intersection of policy-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 (e.g., sensor networks)
- Scalability and performance of PKI 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, signatures, encryption, use of multiple private keys, and selective disclosure
- New paradigms in PKI architectures

### Deadlines for conference paper and panel submissions are:

**Papers and Proposals Due:**  
**October 22, 2006**

**Authors Notified:**  
**December 18, 2006**

**Final Materials Due:**  
**February 26, 2007**

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.

Submissions will be handled electronically. Detailed submission instructions can be found at the workshop website (see <http://middleware.internet2.edu/pki07/>).

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 pre-proceedings at the workshop and in a final proceedings shortly after the workshop.

## PROGRAM COMMITTEE

Kent Seamons, *Brigham Young University* (chair)  
Peter Alterman, *National Institutes of Health*  
Bill Burr, *NIST*  
David Chadwick, *University of Kent*  
Joe Cohen, *Forum Systems*  
Carl Ellison, *Microsoft*  
Stephen Farrell, *Trinity College Dublin*  
Richard Guida, *Johnson & Johnson*

Peter Gutmann, *University of Auckland*  
Russ Housley, *Vigil Security, LLC*  
Neal McBurnett, *Internet2*  
Clifford Neuman, *University of Southern California*  
Eric Norman, *University of Wisconsin*  
Tim Polk, *NIST*  
Scott Rea, *Dartmouth College*  
Ravi Sandhu, *GMU; TriCipher*

Krishna Sankar, *Cisco Systems*  
Stefan Santesson, *Microsoft*  
Frank Siebenlist, *Argonne National Laboratory*  
John Sabo, *Computer Associates*  
Sean Smith, *Dartmouth College*  
Von Welch, *NCSA*  
Stephen Whitlock, *Boeing*  
Michael Wiener, *Cryptographic Clarity*

*General Chair:*  
Ken Klingenstein  
Internet2  
[kjk@internet2.edu](mailto:kjk@internet2.edu)

*Program Chair:*  
Kent Seamons  
Brigham Young University  
[seamons@cs.byu.edu](mailto:seamons@cs.byu.edu)

*Steering Committee Chair:*  
Neal McBurnett  
Internet2  
[neal@bcn.boulder.co.us](mailto:neal@bcn.boulder.co.us)

*Local Arrangements Chair:*  
Sara Caswell  
NIST  
[sara.caswell@nist.gov](mailto:sara.caswell@nist.gov)