

## **PKI – The Gap Between Products and Standards Panel Proposal**

Panel Chair: Santosh Chokani, CygnaCom Solutions

**Panelists:**

Sharon Boeyen, Entrust

Patrick Cain, BBN Technologies

Warwick Ford, Verisign

W. Timothy Polk, National Institute of Standards and Technology

**Session Abstract:** Many Government agencies and private sector companies are exploring the use of Public Key Infrastructure Technology to provide the security foundation for their electronic commerce applications and other information technology needs. As they explore the technology through pilots and small-scale production use, users often want solutions built to standards but standards supporting PKI technology are still emerging. At the same time, vendors are developing PKI products and services for today's electronic commerce applications. It can be costly to update PKI solutions when standards change; yet new standards are developed to provide new functionality. New features in PKI standards can also create greater complexity; yet many commercial offerings still implement only basic functionality.

The purpose of this session is to explore issues related to this evolution process by providing perspectives from the standards community and from the vendor community. Panelists will discuss why they believe PKI standards are changing. They will also describe why they believe some products and services do implement standards and why some vendors implement their own solutions. The panelists will also be asked to compare the security and cost implications of building standards based PKI solutions and proprietary approaches. As a related issue, panelists will provide their perspective on the interoperability implications between products and services as PKI standards continue to emerge. Finally, each panelist will discuss the future of PKI standards and project what, if any, non-traditional PKI standards approaches may be viable in future PKI products and services.

Location: Hyatt Regency Crystal City, Arlington, VA

National Information System Security Conference (NISSC)

## Biographies

Santosh Chokhani is the founder and CEO of CygnaCom Solutions Inc., a small high-technology company specializing in PKI. He also directs the CygnaCom's NVLAP accredited independent laboratories for FIPS 140-1 and Common Criteria Evaluation. He has a Ph.D. in EE from Rutgers University.

Sharon Boeyen is the Technical Director of Entrust Worldwide for Entrust Technologies where she is responsible for the technical and interoperability aspects of Entrust Worldwide. In addition, she provides consulting service, primarily in the area of security and directory standards, to the Entrust development team. Ms. Boeyen has 13 years experience in international standards and has held numerous leadership positions in various forums. Currently, she is the editor of X.509 extension work progressing standards in the areas of privilege management and revocation, and lead editor of the IETF PKIX RFCs profiling the LDAP protocol and schema for use with PKI.

Patrick Cain is a principal member of the technical staff at the BBN Technologies Unit of GTE Internetworking. Mr. Cain provides consulting and guidance to both internal and external clients on the realistic use of security technologies; is a member of the GTEI Security Practice Center; and supports the CTO Office of GTE Cybertrust. In Mr. Cain's 18 years at BBN, he was the lead engineer of the MISSI CAW, was the architect of the BBN SafeKeyper®, represents GTEI in the ANSI X9F standards group, and is the co-chair of the IETF's Secure Time working group.

Warwick Ford, is Chief Technology Officer at VeriSign, Inc. Verisign is a provider of public-key infrastructure solutions for e-commerce, enterprises, and the public. Dr. Ford is a recognized authority on the use of public-key technology, and led the development of digital certificate standards in ISO and the Internet community. He is co-author of the 1997 Prentice Hall book "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption."

Tim Polk has been a member of the Computer Security Division at NIST for nine years, and has been a senior member of the PKI Project Team for four years. He currently edits several IETF PKIX documents, leads NIST's Minimum Interoperability Specifications for PKI Components (MISPC) projects, and is a member of NIST's S/MIME project team.

## Point of Contact Information

Santosh Chokhani  
President  
CygnaCom Solutions  
Suite 100 West  
7927 Jones branch Drive  
McLean VA 22102  
Tel: (703) 848-0883  
Fax: (703) 848-0960  
E-mail: [chokhani@cygnacom.com](mailto:chokhani@cygnacom.com)

Sharon Boeyen  
Technical Director, Entrust Worldwide  
Entrust Technologies  
750 Heron Road, Suite E080  
Ottawa, Ontario  
Canada K1V 1A7  
Tel: (613) 247-3181  
Fax: (613) 247-3690  
E-mail: [sharon.boeyen@entrust.com](mailto:sharon.boeyen@entrust.com)

Patrick Cain  
BBN Technologies  
Tel: (617) 873-2923  
E-mail: [pcain@bbn.com](mailto:pcain@bbn.com)

Warwick Ford  
Verisign, Inc.  
301 Edgewater Pl, Suite 210  
Wakefield, MA 01880  
Tel (781)245-6996 x225  
Fax (781)245-6006  
Email: [wford@verisign.com](mailto:wford@verisign.com)

W. Timothy Polk  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 8930  
Gaithersburg, MD 20899  
Tel: (301) 975-3348  
Fax: (301) 948-1233  
E-mail: [wpolk@nist.gov](mailto:wpolk@nist.gov)