



# THE 1997 RSA DATA SECURITY CONFERENCE

## SPEAKER BIOGRAPHY

### STANDARDS TRACK

PKCS: The Next Generation -  
with a Progress Report on PKCS#11

Speaker: **Ray Sidney**

Research Scientist

RSA Laboratories

100 Marine Parkway Suite500

Redwood City, CA 94065 ,

Phone: 415-595-7703 Fax: 415-595-4126

Email: ray@rsa.com

### Company Background:

RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics Technologies, Inc., is the world's brand name for cryptography, with more than 75 million copies of RSA encryption and authentication technologies installed and in use worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ITU-T, ISO, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. The company develops and markets platform-independent developer's kits and end-user products, and provides comprehensive cryptographic consulting services.

### Presentation Overview:

This talk will summarize the proposed improvements to the Public-Key Cryptography Standards (PKCS) six years after their initial publication. In addition, Dr. Sidney will report on the progress of revisions to PKCS#11/Cryptoki, the programming interface for portable cryptographic devices, such as smart cards and PC cards, developed by RSA Laboratories in conjunction with security vendors.

### Speaker Background:

Ray Sidney received his A.B. in mathematics from Harvard College in 1991 and his Ph.D. in mathematics from MIT in 1995. He joined RSA Laboratories as a research scientist in the fall of 1996. His primary research interests are cryptography, complexity, information theory, and probability.

**PRESENTATION**