



THE 1997 RSA DATA SECURITY CONFERENCE

SPEAKER BIOGRAPHY

STANDARDS TRACK

IEEE P1363: A Comprehensive Standard for Public-Key Cryptography

Speaker: **Burt Kaliski**

Chief Scientist RSA Laboratories

East 20 Crosby Drive

Bedford, MA 01730

Phone: 617-687-7057; Fax: 617-687-7019

Email: burt@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:

IEEE P1363 is a working group started in 1993 to develop comprehensive standards for public-key cryptography based on RSA, Diffie-Hellman and related algorithms. This talk will survey progress in the development of IEEE P1363 in the past year, give an overview of the current draft, and summarize the issues remaining before completion of the standard.

Speaker Background:

Burt Kaliski is Chief Scientist at RSA Laboratories, and serves as chair of IEEE P1363. Dr. Kaliski received B.S., M.S., and Ph.D. degrees in computer science from MIT in 1984, 1987, and 1988 respectively. In 1989 he joined RSA Data Security. His research interests include cryptography and fast arithmetic techniques. He was a Visiting Assistant Professor at Rochester (New York) Institute of Technology during 1988-89. Dr. Kaliski is a member of the IEEE Computer Society, the International Association for Cryptologic Research (IACR), Sigma Xi, and Tau Beta Pi. He is also chair IEEE P1363, a working group developing standards for public-key cryptography, and is program chair of CRYPTO '97.

PRESENTATION