



THE 1997 RSA DATA SECURITY CONFERENCE

SPEAKER BIOGRAPHY

CRYPTOGRAPHERS' TRACK

IBM's Key Recovery Initiative

Speaker: **Stephen Matyas**

IBM Senior Technical Staff Member

IBM Corporation

522 South Road Dept. P330 Bldg. 705

Poughkeepsie, NY 12601-5400

Phone: 914-435-6953

Fax: 914-435-7029

Email: smatyas@vnet.ibm.com

Company Background:

The IBM Corporation has been a leader in cryptographic research and development in the computer industry for more than 25 years. After developing the DES concept and standard the company has produced many hardware and software solutions implementing this and other standards.

Presentation Overview:

In part 1 of the presentation, we provide a high-level design rationale for a cryptographic architecture. We provide typical application scenarios that illustrate how architected cryptographic system has an associated control vector. The control vector defines key usage and prevents abuses and attacks against the key.

In part 2 of the presentation, we provide the design rationale for IBM's key recovery initiative. We describe a key recovery framework that seeks to provide a commercially acceptable solution to governments' needs for authorized access to encrypted data.

Speaker Background:

Dr. Stephen Matyas has been in the forefront of cryptographic technology development for more than 20 years at IBM. Dr. Matyas holds more than 60 patents, has published many articles on cryptography and is co-author of "Cryptography - A New Dimension in Computer Data Security"..

PRESENTATION