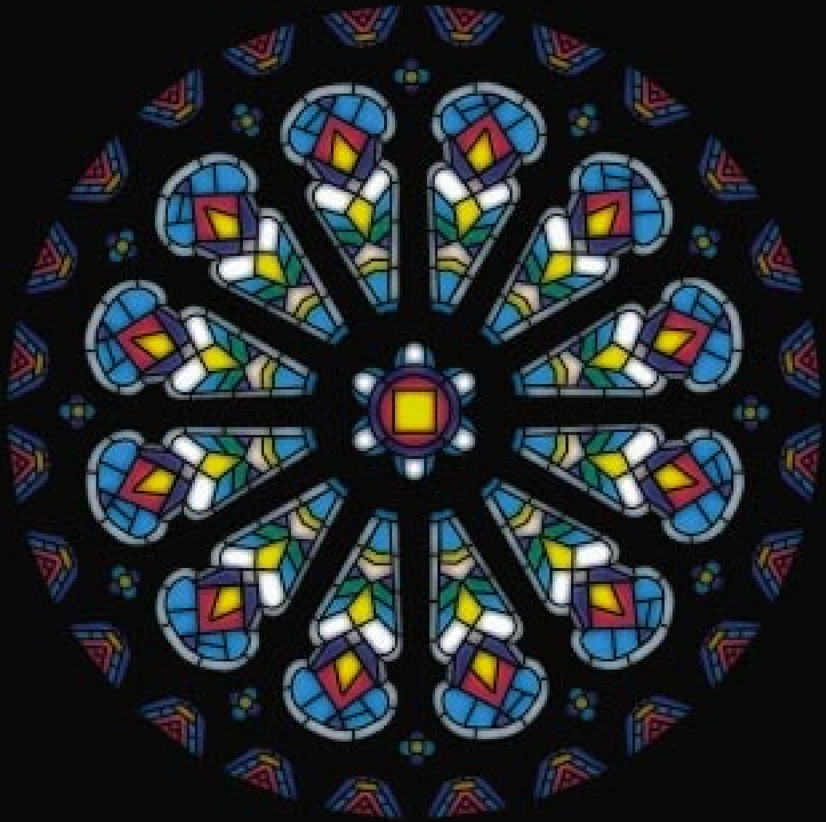


The sine-qua-non event of the crypto community...

SAN FRANCISCO JANUARY 13 - 16

The 1998 RSA Data Security Conference™

In 1518, a Benedictine monk named Johannes Trithemius wrote Polygraphiae, the first published treatise on cryptography. Later, his text Steganographia described a cipher in which each letter is represented by words in successive columns of text, designed to hide inconspicuously inside a seemingly pious book of prayer. Polygraphiae and Steganographia attracted a considerable amount of attention not only for their meticulous analysis of ciphers but more notably for the unexpected thesis of Steganographia's third and final section, which claimed that messages communicated secretly were aided in their transmission by a host of summoned spirits. As might be expected, Trithemius's works were widely denounced as having magical content — by no means an unfamiliar theme in cryptographic history — and a century later fell victim to the zealous flames of the Inquisition during which they were banned as heretical sorcery.

Cryptographers have also historically tended to "cloister" themselves, gathering in small, elite communities of the learned. But times have changed: the dark ages of isolation are ending, thanks to the emergence of the global Internet. And while the Net brings us all closer together, we've also learned that life outside has its risks.

Nearly two decades ago, RSA's founders invented the first practical public key cryptosystem, and ever since, our technologies have defined the perfect balance between openness and control. What began in 1991 as a fifty-person developers' meeting is now the single largest cryptography event of the year. We hope that by gathering together, we can share some of what we've learned over the past year, and go back home able to make life on the Net just a little bit safer.

As such, we invite you "back to the abbey" to join with others who share a love of cryptography, at this, our seventh annual Conference.

Seminars and Exhibits

Recognized by the industry as the largest and most important computer security event of the year, the RSA Conference has three main components: General Sessions, Exhibits, and Class Tracks.

MONDAY JANUARY 12	TUESDAY JANUARY 13	WEDNESDAY JANUARY 14	THURSDAY JANUARY 15	THURSDAY JANUARY 15
Press conferences all day at the Fairmont	Conference opens 9:00 a.m. GENERAL SESSIONS Evening: Reception	CLASS TRACKS EXHIBITS OPEN	CLASS TRACKS EXHIBITS OPEN Evening: Gala	GENERAL SESSIONS Conference closes 3:00 p.m.

The **General Sessions** open and close the Conference, gathering 3,000 attendees together in San Francisco's historic Masonic Auditorium for special keynote addresses, expert panels, and discussions of general interest.

This year's **Exhibits Floor** will feature over 30,000 square feet of vendors demonstrating hundreds of the very latest crypto-enabled products.

Finally, seven simultaneous **Class Tracks** on Wednesday and Thursday will feature a wide variety of tutorials, workshops, seminars and talks. The Conference offers a catalog of over 100 classes, grouped as follows:

- Analysts' Track: topics of interest to industry analysts, public-interest groups, lawmakers and the media
- Cryptographers' Track: for mathematicians, academics and researchers
- Developers' Track: classes for developers and programmers working with crypto
- Products Tracks: two tracks of demonstrations and OEM product pitches featuring the latest crypto-enabled products
- Standards Track: discussions involving international, industry and domestic standards bodies and efforts
- RSA Workshops: an intensive one-day immersion program for developers working with RSA toolkits and crypto engines

Participating Organizations

The annual RSA Conference is unique in the disparate communities that it gathers together. Here you'll find business people, mathematicians, scientists, lawmakers and developers all engaged in lively debate and serious discussion.

You'll meet the best and brightest in fields like:

- Mathematics and Cryptography
- Internet Electronic Commerce, EDI and the Web
- Intellectual Property Protection, Copyright and Net Law
- Federal Cryptography Policy and Standards
- Privacy and Civil Rights

In addition, some of the hottest security vendors will be available to answer questions and demonstrate hundreds of secured products on our exhibits floor. Some current and past participants include:

IBM
Microsoft
AT&T
intel
VeriSign
Open Market
I E T F
NETSCAPE
CyberCash
GTE
Bellcore
Entrust Technologies
Intuit
SPYRUS
MIT
Deloitte & Touche
SRI International
NTT
digicash
TimeStep
VeriFone
ITU Technologies
HEWLETT PACKARD
NASA
Sun
ROBERTSON STEPHENS & COMPANY
NIST

Conference Sponsors

Without the support of several major sponsors, the annual RSA Conference would be impossible.
Please join us in showing appreciation for our partners:

IBM

SecurityDynamics.

Security Dynamics designs, develops, markets, and supports a family of security products that protect and manage access to computer-based information resources. Security Dynamics is the market leader in providing smart card systems that verify the identity of authorized users and prevent unauthorized access to information on computers and networks.

IBM's commitment to securing e-Business starts at the top. To quote IBM Chairman Louis V. Gerstner, "More than any other single factor, the potential of e-commerce hinges on people's confidence that the network can keep confidential transactions confidential, and private records private." IBM creates the industry's most advanced secure information technologies, including computer systems, software, networking systems, storage devices and microelectronics.

RSA Data Security.
A Security Dynamics Company

RSA Data Security develops and markets platform-independent developer's kits and end-user products, and provides comprehensive cryptographic consulting services. RSA's technologies are part of existing and proposed standards for the Internet and World Wide Web, CCITT, ISO, ANSI, IEEE, and business, financial and electronic commerce networks around the globe.

GTE

GTE, with annual revenues and sales exceeding $21 billion, is one of the largest publicly held telecommunications companies in the world. Through its commitment to CyberTrust, GTE realizes the Internet's importance and potential as a powerful communications medium for both businesses and individuals. CyberTrust draws on GTE's broad experience to provide you the best value possible.

TimeStep

TimeStep Corporation produces secure virtual private networking (VPN) solutions that make the Internet a safe place for data. Using TimeStep's PERMIT™ technology, businesses can send sensitive data across the Internet confident that it will travel safely-unseen, unchanged, uncopied, and intact. PERMIT technology transforms the Internet into corporate intranets and extranets.

Check Point
Software Technologies Ltd.

Check Point Software Technologies Ltd. provides software products that allow businesses to implement Internet and Intranet connectivity solutions with full security. Check Point Software's flagship product, Check Point FireWall-1, has emerged as the standard for enterprise-wide network security. We protect thousands of organizations worldwide from unauthorized internal and external access.

Rainbow
Technologies
Internet Security Group

Established in 1984, Rainbow Technologies provides security solutions for the information age. Rainbow is the world's leading developer, manufacturer and supplier of software protection solutions, and a leading provider of network license management, Internet and information security.

Analysts' Track

Topics of interest to analysts, public-interest groups, lawmakers and the media

A Worldwide Survey of Cryptographic Products
David Balenson, Trusted Information Systems

An update on TIS's ongoing comprehensive survey of the rapidly accelerating worldwide availability of hardware and software products employing cryptography, with the latest results, newest products, and current trends. (2)

PANEL: Cryptography, On-Line Loyalty and the Exchange of Near Money Currencies
Bradley Crooks, Saatchi & Saatchi, London
Oscar W. Jenkins, Uptime Group Plc.
Dr. Vaclav Matyas, University of Cambridge

Powerful economic forces combined with the main stream use of PKI will soon result in free trade of corporate "Loyalty and Incentive" points on-line. (1)

Hidden Flaws
Paul Kocher, Cryptography Research

There are two measures of a cryptosystem's security: the level of security it is designed to provide, and the probability that the system is weaker than expected. This talk explains why serious security flaws are so common and how to indentify and avoid them. (2)

Legal Issues for Companies Outsourcing CA Services
Andrew R. Basile, McBride Baker & Coles

Laws are being enacted throughout the country and the world impacting the deployment of digital certificates. This presentation summarizes the latest developments, focusing on the various regulatory models that have been proposed and the sometimes controversial policies underlying those models. (2)

PANEL: Accreditation of Security Products
John Morris, CygnaCom Solutions, Inc.
Leo Pluswick & Frederick G. Tompkins, NCSA

The cryptographic marketplace discriminator now hinges on technical product certifications. This presentation provides an in-depth look at Cryptographic Algorithm Conformance (RSA, DSA, ECDSA), Certificate Authority Accreditation, the NVLAP NSA RSA logo programs, EDAP, MISPC, TPEP, and TTAP. (2)

PANEL: International Standards for Authentication of Electronic Communications: Are They A Necessity?
Alexander Blumrosen, Bernard-Hertz-Bejot, Paris
Richard Allen Horning, Tomlinson Zisko Morosoli & maser LLP
Adrian Lifely, Osborne Clark, London

The participants in this panel discussion, all legal experts on electronic commerce, will underscore the great differences in national laws on the subject, and discuss the status of the international efforts to develop authentication standards, where new twists occur almost daily. (2)

PANEL: Crypto and the Media
Sasha Cavender, IPO
Simson Garfinkel, Boston Globe
Dan Gillmore, San Jose Mercury News
John Markoff, New York Times

Four journalists look at cryptography and the media, and ask why the media too often get things wrong when covering crypto — and offer suggestions on how the cryptography community can help journalists do a better job. (1)

The FBI's Infrastructure Threat Assessment Center
Kenneth M. Geide, Federal Bureau of Investigation

The FBI's Computer Investigations and Infrastructure Threat Assessment Center (CITAC) initiative and its impact on FBI investigations, training and crime prevention efforts; encryption in FBI outreach and investigative endeavors; and the use of encryption by "bad actors" as seen through FBI CITAC investigations. (2)

A Web Implementation of the NRC's National Recommendations for Protecting Health Information
Dr. John D. Halamka, Harvard Medical School

We demonstrate a balance between ease of use and confidentiality in a World Wide Web implementation of the National Research Council's recommendations for protecting electronic health information, created using commercially-available, standard components. (2)

Liability and Other Legal Issues Relating to the Development and Use of Encryption Technology
Gregg Kirchhoefer, Kirkland & Ellis

Greg Kirchhoefer and Adam Petravicius, respectively partner and associate at the law firm of Kirkland & Ellis, address legal issues connected with data security; in particular, the potential liabilities faced by product developers and persons failing to use adequate data security measures. (2)

The Development of a Global Digital Signature Law
Michael Baum, VeriSign, Inc.

The United Nations Commission on International Trade Law has initiated the development of model legislative provisions focused on secure electronic commerce. This session explains the current U.N. initiative to develop a model law focused on digital signatures, certificates, secure electronic commerce, and possibly other mechanisms. (3)

Getting Management Buy-In on Encryption
John G. O'Leary, Computer Security Institute

Those who would develop and implement successful encryption-based security solutions must understand the mind-sets and thought processes of the managers who approve these solutions and the users who are directly affected. This session provides ways to get "them" to buy-in on these solutions. (1)

PANEL: Smartcards Update
Bill Powar, Venture Architects
Murzad Madavi, Slumberger
Ted Goldstein, JavaSoft
Allen Weinberg, First Data

Smart cards are uniquely positioned to provide solutions to the security needs of the evolving world of network computing. Hear how they can be made to work and what the practical issues and impediments are that they have faced to date from people who are implementing smart cards. (1)

True Life Stories of Certificate Authorities in Financial Services
Dr. Stephen Cohn, BBN Corporation

Certification authorities are proliferating, successfully supporting electronic commerce solutions across many industries. Here are case studies of CA's set up and successfully operated by various financial services organizations. (2)

Cryptographers' Track

Topics of interest to mathematicians, researchers and academia

On the Continuum Between On-Line and Off-Line E-Cash Systems
Yacov Yacobi, Microsoft Corporation

Recently a few e-cash systems where proposed that use randomized audit to mitigate fraud. This introduces a new "player" into the game: The audit center. Attacks against it and proper defenses are considered. A curious observation on anonymous payment systems follows. (4)

Design vs. Implementation: Building Implementable Protocols
Dr. Susan Langford, Atalla Corporation

The design of secure cryptographic protocols and their implementation have long been considered independent issues. This session will cover the interrelation of the design and implementation and illustrate how protocol design can make secure implementation more difficult. (5)

Symmetric Block Ciphers
Carlisle Adams, Entrust Technologies, Inc.

This talk will discuss the capabilities of today's symmetric ciphers in terms of speed, key size, flexibility and resistance to known/emerging attacks. Requirements for ciphers of the future, including AES, will be presented along with methods to meet these needs. (2)

Distributed Signing For Certification Authorities
Ernest Brickell, CertCo

At CertCo, we have implemented a distributed signing process that enables the private signature key to be divided into fragments. In this talk, we will review the properties of different methods of distributed signatures for different digital signature algorithms, including security and implementation issues. (3)

Implementaion of Proactive Threshold Public-Key Protocols
Victoria Hamilton, Sandia National Laboratories

Recent papers have described techniques for generating organizational digital signatures that are somewhat resistant to adversarial attacks. This presentation will describe work done at Sandia National Laboratories in implementing both proactive RSA and DSA. (4)

Secure Payments over the Internet
Amir Herzberg, IBM Corporation

A technical survey of recent advancements in securing Internet-based payments. (4)

SPEKE: A Public-key Method for Shared Secret Authentication
David Jablon, Integrity Sciences, Inc.

Extended password-authenticated key exchanges including SPEKE and OKE are described and compared to Bellovin & Merritt's Augmented-EKE. These use hashed verifiers to prove knowledge of a password over the network, without the eavesdropper attack of challenge/response methods, and without predistributed public keys or certificates. (4)

Smart RSA Acceleration on Smart Cards
Francoise Levy-dit-Vehel, GEMPLUS Card International, France

Various algorithmical tricks that optimize the implementation of an RSA signature scheme based on a modulus with three prime factors, and an analysis of the security of RSA in a 3-factor setting. This underlines the extreme suitability of the RSA cryptosystem to drive RSA implementation platforms. (4)

Deterrence Measures for Spam
Kevin McCurley, IBM Research

The Internet has recently seen an explosion of unsolicited e-mail for the purpose of advertising (sometimes called Spam). This talk will survey the different approaches to controlling spam, and propose a new method based on cryptography and electronic commerce. (3)

The Rise of Approximation Attacks
Luke O'Connor, IBM Research Division, Zurich Research Laboratory

Approximation attacks in cryptography use partial information to determine definite information about the key a cipher is using. Two common examples are differential and linear cryptanalysis. This presentation surveys the basic principles of approximation attacks, and how they have influenced modern cipher design. (5)

"Crowds": A New System for Anonymous Transactions on the Web
Mike Reiter, AT&T Labs

Crowds is a system developed at AT&T Labs for providing user anonymity on the web. Web servers are unable to learn the true source of a request because it is equally likely to have originated from any member of the crowd. (3)

Strong Primes
Bob Silverman, RSA Laboratories

The security of the RSA system depends in particular on how one generates prime numbers. This talk surveys the requirements for RSA key generation, and presents an efficient algorithm, which is included in a forthcoming ANSI standard, for generating keys that meet those requirements. (5)

Imprinting of Digital Video
Tamir Tassa, Algorithmic Research Ltd.

A method for fighting coalition-based piracy in digital video distribution systems is discussed. (4)

Performance Comparison of Public-Key Cryptosystems
Michael Wiener, Entrust Technologies, Inc.

To choose among the leading candidate public-key algorithms (RSA, DSA, Diffie-Hellman, and Elliptic Curve Cryptosystems), one must consider their performance for the public-key functions of digital signatures, encryption and key exchange. (3)

LEGEND:

A Worldwide Survey of Cryptographic Products
David Balenson, Trusted Information Systems

A two-year update on TIS ongoing compreshensive survey of the rapidly accelerating worldwide availability of hardware and software products employing cryptography, with the latest results, newest products, and current trends. (2)

Developers' Track

Topics of interest to developers working with cryptography

Survival Guide for the PKI Architect
Judith Furlong, The MITRE Corporation

Many pitfalls are encountered during the design and implementation of a Public Key Infrastructure. Drawing from practical PKI development experience, this session identifies design and implementation challenges encountered by PKI architects and provides advice on how to address these problems. (4)

Hacker Tools and Techniques
Cynthia Cullen, BELLCORE

The latest trends and techniques used by hackers are discussed and demonstrated. Attacks such as denial-of-service, IP hijacking, Trojan horses, network and system monitoring tools are reviewed. Demonstrations include Ping-of-Death, TCP SYN flood, Java and web attacks. (3)

Smartcard Enabled Solutions for Enterprise, Extranet and Intranet Security
Eric Greenberg, Litronic, Inc.

Development techniques leveraging open smartcard standards, including PC/SC and PKCS#11, will be presented. Smartcard development tools based on Java, c, CryptoOS, and Active-X will be presented. Smartcard management methods including user profile management, LDAP, secure isolated security officer stations, and other approaches will be presented. (3)

Autonomous Security Agents: Negotiating Compatible Crypto Protocols on Behalf of the End-User
Hu Yuh-Jong, National Chengchi University, Taipei

We discuss an autonomous software program that provides services that acts on behalf of the end-user to negotiate compatible security protocols.(4)

Extending Cryptographic Services for Network Security Protocols
Bronislav Kavsan, Information Resource Engineering (IRE)

The Network Security cryptographic services are based on extending functionality of the Microsoft CryptoAPI Cryptographic Service Provider (CSP). In addition to utilizing CSP in the form of the DLL, the CryptoAPI - compliant Kernel-Mode driver is implemented to support a wide range of cryptography. (4)

Hardware Cryptography: Selecting the Right Tool for the Right Job
Dr. Susan Langford, Atalla Corporation

This session will reveiw the various categories of cryptographic hardware for application developers. The goal is to provide enough information so that developers can evaluate which type of cryptographic hardware is appropriate for a given application. (5)

UNIX and NT Systems Security Interoperability
Cheri Dowell, Sun Microsystems, Inc.

The Security Interoperability technology addresses the need for reliable inter-working between UNIX and NT. The emphasis is on merging the respective systems as used in real world enterprises, to achieve truly integrated authentication, encryption, access rights, credentials and digital signatures solutions. (1)

Java Cryptography Extension (JCE)
Jan Luehe, JavaSoft

This talk will provide an overview of the Java Cryptography Extension (JCE), including highlights of the new features added since the release of JCE1.1-alpha-1 in May 1997. (4)

Using PKCS #11 in Real Life Applications
Robert Relyea, Netscape Communications

Communicator is one of the first major applications to use PKCS #11 for it's crypto needs. This paper describes how PKCS #11 is used within Communicator as well as Netscape Server products to access to plugable crypto providers. (4)

Commercial Cryptography: Opportunities, Threats and Implementations
Bruce Schneier, Counterpane Systems

Cryptography has become the enabling technology of computer networks. I'll discuss the future of cryptography: technologies, risks, and business opportunities. I'll also examine some of the common mistakes companies make implementing cryptography, and give tips on how to avoid them. (1)

Metadata and Data Labels
Dr. Frank P. Stelmack, Tasc, Inc.

The secure production and distribution of data using data warehouses with Internet gateways is national priority. An abstract architecture is defined and it is shown how metadata can be enforced to secure both data productiion and data distribution. (2)

Anonymous Collaboration
Warren Stringer, TestDrive Corp.

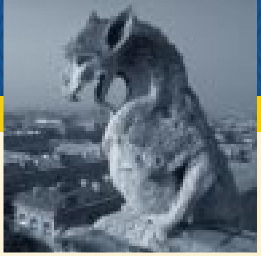
Explore the balance between private exploration and group interaction. Transform the effectiveness of Email, newsgroups, search engines, groupware, and collaborative filtering. Special focus on passive collaboration. (3)

Implementation of a Cascading Random Number Generator
David Grawrock, Symantec

This talk will cover cascading random number generators. This technique makes an attackers job of determining what the seed of the random number generator was much more difficult. (3)

Standards Track

Discussions of international and domestic standards bodies and efforts



PANEL: S/MIME - The Next Generation
Dr. Carlisle Adams, Entrust Technologies, Inc.
Paul E. Hoffman, Internet Mail Consortium

The S/MIME standard is being extended to handle such useful features as signed receipts, secure mailing lists, and security tags. This panel will give an overview of the current and planned extensions to S/MIME and their status. (2)

The SET Root Certification Authority
Mark Jefferson, CertCo

MasterCard/VISA, in their SET PKI, have the most demanding requirements for root key management of any PKI now in implementation. This talk will describe the how and why of CertCo's winning product architecture, and raises the bar for similar products. (2)

The IETF's PKIX Working Group: An Update
Dr. Carlisle Adams, Entrust Technologies, Inc.

This seminar will provide an overview of the current activities of the PKIX IETF Working Group. It will also highlight the importance of the group; industry and government support for the organization; and the status of each PKIX activity within the Internet standardization process. (2)

PANEL: Transport Layer Security
Christopher Allen, Consensus Development Corporation

Transport Layer Security (TLS) 1.0 is the IETF's open successor to the widely deployed SSL 3.0 standard. Participants will receive an overview of the changes between SSL and TLS, the current status of TLS efforts, future changes under consideration, and TLS enabled products. (3)

Java Based Secure DNS Server
Ashar Aziz, Sun Microsystems

The design and implementation of a Java based extensible and secure DNS server is described. Use of Java provides for the naming scheme to be run-time and boot time extensibile permitting addition of new DNS records types at run time. (3)

International Cryptography Standards
Dr. Santosh Chokani, CygnaCom Solutions

This talk describes the enhancements to the International Common Criteria Standard to allow for evaluation of products (such as BSAFE) and systems containing cryptography. (1)

PANEL: Achieving Interoperability within the Public Key Infrastructure
Donna Fogle Dodson, Tim Polk, NIST
Warwick Ford, VeriSign, Inc.

Certification authorities are now a reality, and they are enabled through several separate venues. However, the need for complete interoperablility still persists. This presentation explores issues of trust, policies, and practices, PKI-firewalls, and the need for standards to support roles and authorization. (2)

A Current Overview of IPSEC
Dr. Stephen Kent, BBN Technologies

The IPSEC standards offer IP layer security services for a wide range of applications. This presentation examines how IPSEC is used to create virtual private internets, protect remote user communication, and to strengthen the access control features of firewalls. (3)

Introduction to SSL 3.0
Paul Kocher, Cryptography Research

In this talk, Paul Kocher, the cryptographer responsible for SSL 3.0, will provide a high-level introduction to the protocol, covering issues such as certification, cryptographic security, key management, cipherspec and ciphersuite selection, export restrictions, and SSL 2.0 interoperability. (3)

ANSI and ISO Crypto Standards: A Progress Report
Sandra Lambert, Lambert & Associates

ANSI and ISO standards-making bodies develop the drafts which affect our corporate and personal lives. This session provides an overview of the currently published crypto standards, those in progress and on the drawing board, plus the market and geo-political factors influencing their development. (2)

Lessons Learned in CA Accreditation and Assessment
Eric V. Leighninger, Deloitte & Touche Security Services

Deloitte & Touche Security Services LLC has conducted certification authority (CA) assessments for both a private and a public CA for NETDOX, Inc. This presentation outlines lessons learned and discusses key technical issues associated with CA assessments and accreditation for electronic commerce applications. (2)

International CA Cross Certification
Yoshito Nakamura, Mitsubishi Corporation

JapanNet and CommerceNet have been collaborating to conduct the world's first cross certification pilot involving two Certification Authorities (CAs) in USA and Japan. Mitsubishi Corporation and a US Trading Partner are using the certificates issued by their respective CAs to supprt international EC Transactions. (2)

PANEL: NIST Standards Developments and Activities
Edward Roback, Miles Smid, NIST

This presentation wil focus on NIST's cryptographic standards activities, including the competition to select an algorithm for the Advanced Encryption Standard, plans to develop a public key based key agreement and exchange standard and include additional algorithms in the federal Digital Signature Standard. (1)

Using PKCS #11 to Support Multiple Cryptographic API's
Gregg Weissman, SPYRUS

This workshop examines a universal CAPI object model designed to support three major cryptographic API's with maximal reuse of design and code. Using this model leverages the API's core commonality, using PKCS#11 as a basic infrastructure. (4)

Talk Title
Speaker

Description

Technical Level
(5 = most technical)

NOTE: Speakers and schedule are subject to change without notice

Products 1 Track

Talks and demos featuring the latest crypto-enabled products

NetDox: The World's First Global Service for Confidential Digital Communications
Julie Grace, NetDox, Inc.

NetDox has created an environment for the interoperability of digital certificates on a worldwide basis to enable commercial grade commerce with confidentiality over the Internet. The NetDox service has created the first general commercial consumer demand for individual digital certificates.

Norton Your Eyes Only Version 5
David Grawrock, Symantec

This talk will cover the new features of Norton Your Eyes Only. A description of how NYEO does on the fly encryption along with the full administration of public and private keys is covered. NYEO will be demonstrated. (1)

Security on a Java Smart Card
Dr. Scott Guthery, Schlumberger

The secure computing features of the Java programming language are combined with the software and hardware features of a smart card to provide a secure and very portable personal computer. (1)

Securing the Corporate Intranet: The Push Solution
Eli Barkat, BackWeb Technologies

As push technology becomes more widely adopted in corporate intranets, the issue of security increases in importance. If information makes its way outside the firewalls, or information breaks in, the network becomes vulnerable. Learn how to make the Intranet a reliable and secure communications tool. (1)

Secure Remote Access with NetSentry Remote
Ken Biery, Jr., StorageTek Network Systems Group

Secure remote access using a combination of cryptographic methods for data privacy and data integrity. This combination enables road warriors and telecommuters to remotely access the same network services as if they were using a desktop on their traditional LAN segment. (1)

BBN High Assurance CA Solutions
Patrick Cain, BBN Technologies

A short overview of the different models of providing certificates in a Public Key Infrastructure, emphasizing the security and cost differentiators. Includes an update on the new advances introduced in the BBN SafeKeyper Compact CMS PKI product line in 1997. (1)

Enabling Business over Open Networks with Gate Technology
James Chen, V-ONE Corporation

V-ONE's SmartGate seamlessly integrates the critical security components of smart card technology, authentication, encryption and access control into a single product client/server security product. GE Information Services,MCI, Florida State University and most Top Ten banks and financial institutions use SmartGate today. (1)

Digital Signatures and the US Postal Service's Information Based Indicia Program
Donald A. Cole, Booz, Allen & Hamilton

The United States Postal Service Information Based Indicia Program is defining an environment in which customers can apply and digitally sign postage through new technologies. This new technology will aid in improving the security of postal revenue. (1)

Hewlett-Packard's Cryptographic API Strategy
Mike Jerbic, Hewlett-Packard Company

This presentation describes how the strategy's three components, Microsoft Crypto API, Intel CDSA, and GSS-API together form a cryptographic platform for use around the world. By using these components, the platform provides application developers with the widest range of APIs available. (4)

GPK Cards: The Key to Digital Signatures and Secure Electronic Commerce
David M'Raihi, GEMPLUS

The GPK8000 is the new cryptographic smartcard of GEMPLUS' GPK range. In this presentation, we present new implementation tips related to fast and reliable implementations of RSA, including 2048-bit signature and verification using a 1024-bit engine, with various speed and memory trade-offs. (4)

Java Applets and ActiveX Controls on the Corporate I*net Security Issues and Solutions
Ron Moritz, CISSP, CISA, Finjan, Inc.

Addressing security issues with Java applets and ActiveX controls, the risks of executable content, the Java security model and author signing, the basics of using downloadables on the corporate network, suggestions of future directions of executable content, and a review of available solutions. (2)

Ownership Issues and Digital Watermark Technology
Scott Moskowitz, The DICE Company

A comparison on various "digital watermark" systems. Strengths and weaknesses of various systems will be discussed in determining an ideal solution to determining ownership of digitized works. (1)

Datakey Crypto Card Operating System (DKCCOS)
Bill Rohland, Datakey, Inc.

DKCCOS is a leading-edge smart card operating system jointly developed by Datakey, Inc. and Uptronics, Inc. for use in Datakey's SignaSURETM information security solutions. It provides an extended suite of hybrid cryptosystem functions, and compatibility with ISO 7816 and PKCS #11. (3)

Spotlight on SET Hardware Cryptography: Atalla PayMaster
Steve Scott, Atalla Corporation

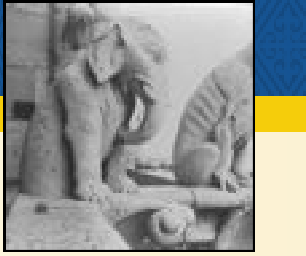
In this session, Atalla will demonstrate the capabilities of its industry leading PayMaster Internet Security Processor. This product is being used in many high-profile Internet commerce pilots by leading card issuers, acquiring banks and technology providers. (2)

High Performance RSA Hardware Accelerator Design
Dr. Shigenori Shimizu, IBM Research, Tokyo Research Laboratory

A discussion of the design of IBM's hardware-based modulo exponentiation accelerator products for System/390 enterprise mainframes. (4)

Products 2 Track

More talks and demos featuring the latest crypto-enabled products



An Overview of CryptoAPI 2.0
Mohan Rao Cavale, Microsoft Corporation

Crypto API 2.0 provides programmer support for key generation and exchange, digital signatures, and data encryption using a provider architecture to support installable Cryptographic Service Providers and certificate management. This talk discusses the new cryptographic functionality available in CryptoAPI 2.0, including certificate management. (3)

Entrust Architecture and Application Solutions
Ian Curry, Entrust Technologies, Inc.

An examination of issues relating to network security and how Entrust Technologies' security software products protect electronic business processes. Entrust software satisfies requirements for which no commercial product currently exists, namely: security solutions that can scale to enterprise levels and work across multiple platforms and applications. (3)

Securing MQ Series Middleware
Barry Ader, Candle Corporation

IBM's MQSeries is the market leader in Messaging Middleware. There are several security areas that an IS organization needs to be concerned with regarding MQSeries. This presentation details those concerns and outlines Candle's MQSecure product that uses RSA cryptography to meet those needs. (1)

A System Level Solution for Virtual Private Networking
Ron Avignone, VPNet Technologies, Inc.

Learn about VPNet's comprehensive product line for extending intranets, providing secure remote access, and forming multi-company extranets over public networks. (1)

The Modular Security Management System (MSMS)
Hany Fahmy, Racal Data Group

A discussion of the architecture of the Modular Security Management Systems (MSMS) which is defined for enterprise network applications. The proposed MSMS can accommodate new security services and new techniques and technologies, providing a common platform that adheres to standard requirements and interfaces. (3)

Integrating Certificate Infrastructures with IPSEC VPNs
Brett Howard, TimeStep Corporation

The IETF has defined a suite of security protocols (IPSEC) for VPNs ranging from key agreement to IP packet encapsulation. Unfortunately, integrating VPN technology into PKIs is not straightforward, both when interfacing to the PKI itself, and when using certificates in conjunction with policy. (2)

Security for Network Computing
Paul Lambert, Oracle

The fusion of object, Internet and client/server technologies in a network-computing architecture presents many new security challenges and solutions. This presentation describes how systems built on a network-computing architecture will speed the deployment of new applications, significantly lower maintenance costs and improve security. (2)

Secure Banking From Your Couch
Patrick Lin, WebTV Networks

WebTV Networks, Terisa Systems and Wells Fargo jointly present a crystal ball description of the future of electronic commerce specifically focusing on home banking via Internet appliances. Panelists will review the current status of security and describe the advances in store. (1)

TRANSACTOR: Electronic Commerce for Digital Objects
Ron Martinez, Transactor Networks, Inc.

Transactor is a new, net-based, secure electronic commerce technology specifically designed to facilitate the new digital object commerce. Transactor allows anyone to create, buy, sell, barter, transact, and authenticate ownership of digital objects. (2)

CryptoSwift: A Necessity for Serious Commerce Servers
Mitch Simon, Rainbow Technologies

Operating a serious commerce or secure server? Come and see Microsoft's IIS web server handling TEN TIMES more customers. We'll show you how CryptoSwift Secure Server Accelerators extend the capacity of your existing server while making it more secure for electronic commerce. (1)

ROSETTA Secure Smart Card and SPYCOS
Rich Skibo, SPYRUS

SPYRUS provides secure end- to-end solutions for OEM's, application developers, and end users. These solutions are developed through strategic partnerships, public key security engineering expertise, toolkits, patented technologies, and flexible product configurations offering form factor independence (PC cards, smart cards) and algorithm agility. (2)

Biometric Encryption for Secure Key Generation
Dr. Colin Soutar, Mytec Technologies

This talk will present an overview of how the process of Biometric Encryption is used in Mytec's fingerprint recognition system, Touchstone. We will present some results on the performance of the system, along with a discussion on the security of the method. (3)

The Development of IBM's Key Recovery Products: Lessons Learned
Narayanan Vasudevan, IBM Corporation

We discuss the lessons learned from developing the IBM SecureWay Key Management framework. Major design requirements included scaleability, evolvability, performance and open architecture. (3)

WorldSecure Server: Comprehensive E-Mail Security and Encryption Policy Enforcement
Reynold Wong, Worldtalk Corporation

Worldtalk presents WorldSecure Server, a comprehensive e-mail security solution that integrates a number of security features in one product, including a server-based S/MIME, virus scanning, access and content controls and desktop encryption policy management. (1)

NOTE: *Speakers and schedule are subject to change without notice*

RSA Workshop

An intensive one-day immersion program for developers working with RSA toolkits and crypto engines

Working with the BSAFE Toolkit
Dung Huynhn, RSA Data Security, Inc.

This presentation will outline how developers can use BSAFE to implement cryptographic constructs. The talk will also include some security issues concerning cryptography and how to address those issues using BSAFE. (3)

Working with the S/PAY Toolkit
Dr. Robert Baldwin, RSA Data Security, Inc.

Few standards have taken off like SET, the RSA-based solution for Internet credit card transactions. Learn how to use the S/PAY toolkit to quickly add SET payment options to your products. (4)

RSA Developer Support Services
Matthew S. Hamrick, RSA Data Security, Inc.

Aimed towards both current RSA Customers and non-customers alike, this talk will present an overview of RSA support and services offerings and delivery options. (1)

PANEL: Working with Hardware Interfaces for RSA Toolkits
Shawn Abbott, Rainbow Technologies
Robert Burroughs, IBM Corporation

A discussion of B/HAPI and other hardware "hooks" available in RSA's BSAFE software developers kit. (3)

Working with the S/MAIL Toolkit
Tim Matthews, RSA Data Security, Inc.

Supported by Microsoft, Netscape, and many others, S/MIME is by far the most widely implemented standard for e-mail security. S/MAIL makes building your own S/MIME application easy.(4)

Working with the J/SAFE Toolkit
Tim Matthews, RSA Data Security, Inc.

This presentation will describe how developers can use JSAFE to implement cryptographic constructs in Java applications. The talk will outline the JSAFE model and give some examples on executing the model. It will also address various issues unique to Java, such as thread-safety, cloning, serialization and protecting memory. (3)

McAfee, RSA, and the SecureONE API
Victor Chang, RSA Data Security, Inc.

SecureONE is intended to provide a broad framework for customers who want to implement integrated security solutions. This framework incorporates the programming interfaces of McAfee's Virus Interface for Protective Early Response (VIPER), Security Dynamics' Enterprise Security Services (ESS), RSA's security engines and VeriSign's Developer Kit (VDK). (3)

Bonus Track

A little of this, a little of that; classes on a variety of topics

Cryptographic Security Services Protocol
Dr. John Brainard, RSA Laboratories

RSA Laboratories is developing protocols supporting a wide range of security services based on cryptography, with the intent of producing an open standard. Support of both X.509 certificates and the emerging SPKI/SDSI initiatives is also envisioned. (4)

Open Commerce SafeXChange
Robert Frank, Open Commerce, Inc.

Description and demonstration of Open Commerce's new S/MIME-based Internet Services and its SafeXChange Intranet Server product which solve EDI entry barriers, allowing users to implement affordable and secure EDI capabilities via the global Intranet. (1)

Security Support and Interoperability in Wireless Networks
Kamran Ghane, Hiva Consulting

Privacy and Authentication have become major concerns in wireless systems. This presentation discusses the current standards suites and security mechanisms used in wireless WANs and LANs. (4)

Designing Secure Systems for Internet Commerce
Win Treese, Open Market, Inc.

Security in Internet commerce requires a comprehensive approach to designing a whole secure system. This discussion will look at where security is required in Internet commerce systems and discuss ways to solve security issues. (3)

Next Generation Netscape Security
Karen Horwitz, Netscape Communications Corporation

Learn how to deploy security solutions using Netscape's latest client and server products. Both overall architecture and technical details will be described. Topics include single-sign-on, security-enhanced messaging, directory integration, strong crypto for export, smart cards, and key and certificate management. (3)

A Certificate Management Protocol for PKIs
Cheryl Madson, Cisco Systems, Inc.

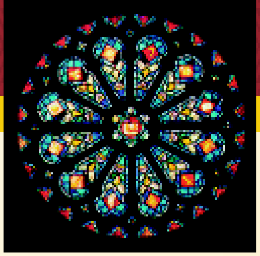
This presentation describes a certificate management protocol, baesd upon various PKCS standards, that PKI clients and Certificate Authority servers can use for certificate life cycle operations such as client enrollment and revocation, and certificate and CRL access. (4)

FIPS 140-1 Certification: The Netscape Experience
John Hines, Netscape Communications

This talk will discuss Netscape's experiences with FIPS-140-1 certification - the work involved (from both non-technical and technical perspectives), the design trade-offs, and the algorithm / implementation changes made in the Security Module 1 cryptographic module to meet the FIPS-140-1 requirements. (3)

Keynotes & General Sessions

Special keynote addresses, expert panels, and discussions of general interest



Welcome
Jim Bidzos, president, RSA Data Security, Inc.

RSA president Jim Bidzos welcomes you to this, our seventh annual conference, recaps the year that was, and offers a preview of some of the more significant events coming up over the next four days.

Cryptographers' Expert Panel
Dr. Ron Rivest, MIT
Dr. Peter Neumann, SRI International
Dr. Whitfield Diffie, Sun Microsystems
Dr. Taher ElGamal, Netscape Communications
Dr. Burt Kaliski, RSA Laboratories

The single highest-rated session of the RSA Conference, six years running! Join the most famous minds in mathematics in a traditional RSA free-for-all. Dr. Peter Neumann of SRI hosts, and no subject is off-limits. And of course, there will even be time for some audience Q&A.

Cryptography, The Renaissance and the Inquisition
Steve DeCaroli, University of Binghamton

Generations of monks like Johannes Trithemius, cloistered in scriptoria, kept the flame of knowledge burning throughout the Middle Ages. But prayer books weren't the only things being transcribed. Our special guest provides a historical perspective on the emergence of Cryptographic texts during one of the most tumultuous periods in Western history.

Why Public-Key Infrastructures Are Necessary to Support Electronic Commerce
John Ryan, Entrust Technologies, Inc.

Security is one of the greatest hurdles in making Internet-based electronic commerce fully viable. Electronic commerce will only become widespread when digital signatures for authentication and encryption for privacy are widely deployed. Only a public-key infrastructure can provide a fully-assured secure transaction.

Washington Update
Cindy Cohn, McGlashan & Sarrail, P.C.
Dr. Dorothy E. Denning, Georgetown University
Bruce J. Heiman, Preston Gates Ellis & Rouvelas Meeds LLP
Susan Landau, University of Massachusetts

From Clipper to the Software Key Escrow Proposal, U.S. cryptography policy has been based on the premise that wiretaps are critical in the fight against terrorism, organized crime, and kidnappings, and that the government cannot afford to lose this tool. Does the government have a case? Hear the evidence and decide.

Encryption Control and Global Security Policy: Is the Conflict in National Legal Regimes Retarding Electronic Commerce?
Richard A. Horning, Tomlinson Zisko Morosoli & Maser LLP
Robert Bond, Audley, Hopkins & Wood
Wilson Wong, Allen & Gledhill

The panelists, all experts on electronic commerce law, will offer their particular perspectives on national encryption policies in the leading "wired" economies, will note the differences in national laws on the subject, and discuss the international efforts to develop common international encryption policy.

Cracking Keys for Fun & Profit. The Year in Review.
Peter Trei, Process Software Corporation

A review of the work done in 1997 in brute-forcing keys, using loosely coupled machines on the Internet. What lessons should system designers learn from these attacks? How are they organized? Are they a realistic threat?

RSA Product Announcements
Scott Schnell & Victor Chang, RSA Data Security, Inc.

Once a year, RSA announces a barrage of new products and technology initiatives at the Conference. Here you'll be among the very first to see RSA'hot new line of crypto tools and end-user products.

The Evolution of Secure Internet Payments
Paul Lampru, VeriFone

Topics include: The Business Case for Internet Commerce - Forecasts of the Value of Payments over the Internet - Consumer Education and Experience with Public Key Encryption - Important Financial Industry Payment Pilots (SET, BITS) for "Haves" - Proposed Internet Payment Systems for "Have-Nots" or EBT - Gradual Displacement of Magnetic Stripe Card Terminals by Chip Card Terminals - Future of Money: Convergence of Virtual and Physical Payment Systems

IBM SecureWay 1998
Kathy Kincaid, IBM

IBM's SecureWay is one of the most complete, enterprise-wide security offerings in the industry, and 1998 will bring some exciting new products and even a few surprises from "Big Blue". See them here first.

Secure Single Sign-on: Using One Password To Navigate the Enterprise
Khris Loux, Security Dynamics Technologies Inc.

This session will examine the elements of secure single sign-on and the integration of discrete security solutions to create a comprehensive, flexible set of security capabilities. As corporations seek to capitalize on the emergence of intranets and extranets, customers want to implement maximum protection for corporate information assets, while maintaining ease of use and administration. Through a discussion of real-world examples, attendees will gain a deeper understanding of why, when and how corporations will implement SSSO technology.

Special Guest Keynotes
To be announced

The 1998 RSA Conference will feature many special surprise guests from the best and brightest in the digital community. Watch our website for details as the conference approaches.

California Academy of Sciences

The California Academy of Sciences is the setting for Thursday night's Gala. Sip champagne and nibble on hors d'oeuvres with us while browsing the spectacular exhibits.
http://www.calacademy.org

Masonic Auditorium

The Masonic Auditorium will host the general sessions on the first and last days of the Conference. See the auditorium (and learn more about the Masons) at
http://www.freemason.org.

The Mark Hopkins

The Mark Hopkins Inter-Continental will host several of the exhibitors and one of the conference tracks on days two and three of the Conference.
http://www.interconti.com

The Fairmont Hotel

The elegant Fairmont Hotel, high atop Nob Hill, is RSA's headquarters during the conference, and plays host to most conference tracks. From \$135^{00}.
Phone: 800/527-4727
http://www.fairmont.com

The Ritz Carlton

Mobil Travel Guide Five-Star, AAA Five-Diamond hotel — ranked San Francisco's best by Conde Nast Traveler readers. From \$150^{00}.
Phone: 800/241-3333
http://www.marriott.com

Renaissance Stanford Court

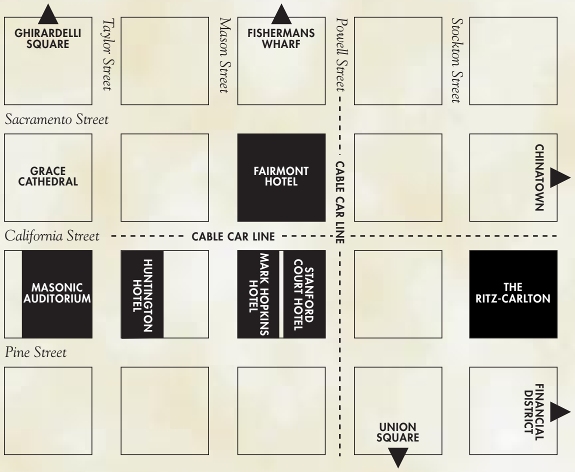
This hotel surrounds guests in elegance, with turn-of-the-century detail, fine antiques, a beaux-arts fountain, and a breathtaking lobby dome. From \$166^{00}.
Phone: 800/227-4736
http://www.renaissancehotels.com

Conference Venues

San Francisco is one of the world's most popular travel destinations: a spectacular city noted for its climate, culture and contrasts. At its heart there lies a special neighborhood which embodies all the city's most beloved qualities: Nob Hill.

The 1998 RSA Data Security Conference will be held at five convenient Nob Hill venues: the Fairmont Hotel, the Mark Hopkins Inter-Continental, the Stanford Court Hotel, The Ritz-Carlton and the Masonic Auditorium. These landmark hotels offer world-class accommodations in a quiet and stately location, yet are just a brief cable car ride away from Union Square, Chinatown, Ghirardelli Square and Fisherman's Wharf.

Special room rates have been negotiated for conference attendees. **Make your reservations by December 1, 1997**, and be sure to mention the RSA Data Security Conference to obtain the discounted rate.



Conference Details

Your attendance fee includes all of the following:

- Four full days of talks, seminars and workshops
- Unlimited access to over 30,000 square feet of exhibits
- Continental breakfasts and full lunches
- Comprehensive conference notes and materials
- A pre-conference welcome reception, Monday January 12
- Admission to the Cryptographers' Gala at the California Academy of Sciences in Golden Gate Park, on Thursday, January 15

Travel Arrangements

United Airlines is offering discounted fares to all RSA Conference attendees. A 5% discount on published fares, including First Class, will be offered on any United, United Express or Shuttle by United flight.

United will also provide domestic freight discounts at a rate of 35% off of bulk rates, 25% off of container rates and 10% off of small package dispatch rates. If you are interested, please provide United the details of your shipping requirements at least 30 days in advance of the actual shipping dates.

Please call the United Airlines Meetings Desk at 800/521-4041 and reference the Meeting ID Code: 516WH. The Meetings Desk is open Mondays-Sundays, 7:00 am - 12:00 midnight (EST).

Avis and Alamo car rental companies will offer discounts of 10% off the applicable rental rates when reservations are made in conjunction with United Airlines reservations.

How to Register

REGISTER ON THE NET

http://www.rsa.com

REGISTER BY E-MAIL

info@lke.com

REGISTER BY TELEPHONE

Call LKE Productions at:
(800) 340-3010 or
(415) 544-9300

REGISTER BY FAX

Photocopy and fax the completed form to:
(415) 544-9306

REGISTER BY MAIL

Photocopy and complete the form, and mail it to:

RSA Conference
c/o LKE Productions
1620 Montgomery Street
Suite 120
San Francisco, CA 94111

Confirmed registrants who cancel prior to the conference or who do not attend the conference will forfeit their entire registration fee. All cancellations must be made in writing. Substitutions, including those made on-site, are allowed at any time with the written permission of the original registrant.

⌘ IMPORTANT: CLASS SIGN-UPS

Once you have registered for the conference, you will receive a confirmation number. **Don't lose this number!** You will need it to sign up for classes. Pre-register for the classes you wish to attend at *http://www.rsa.com/conf98/* or simply call LKE Productions at (415) 544-9300 to receive a class registration form.

Please register early.
The RSA Conference
always sells out.

The 1998 RSA Data Security Conference™

c/o LKE Productions
1620 Montgomery Street, Suite 120
San Francisco, CA 94111

1998 RSA Conference Registration Form

Registrant's Information

Name: ______

Title: ______

Company: ______

Address 1: ______

Address 2: ______

City: ______

State: ______ Zip: ______

Country: ______

Phone: (   ) ______

Fax: (   ) ______

E-mail (required): ______

❑ Check here if you don't wish to be included on the published attendee list

Conference Fees

Your fees include conference proceedings, admission to all general sessions, class tracks and exhibits, as well as breakfast, lunch, and evening cocktail receptions each day.

Early-Bird registration:	**$795**	(postmarked by October 15, 1997)
Discount registration:	**$995**	(postmarked by December 1, 1997)
Standard registration:	**$1,295**	(after December 1, 1997)

(Sorry, since we always sell out, registration will not be available at the door)

Number of people attending: ________ Total amount enclosed: $ __________

Method of Payment

❑ Cashier's or Company Check enclosed
(payable to RSA Data Security, Inc.)

❑ VISA ❑ Mastercard ❑ American Express

Credit Card Number: ______

Expiration Date: ______

Cardholder Name: ______

Signature: ______

Just So We Know:

In which seminar track(s) do you think you will spend most of your time?

❑ Analysts
❑ Developers
❑ Cryptographers
❑ Products
❑ RSA Workshop
❑ Standards

Will you be attending the Welcome Reception on Monday night, January 12?

❑ Yes ❑ No

Will you be attending the gala at the California Academy of Sciences on January 15?

❑ Yes ❑ No

FAX THIS FORM TO 415-544-9306