RSA
DATA SECURITY, INC.
THE KEYS TO PRIVACY AND AUTHENTICATION

Ciphertext

Volume 3, No. 1 Fall 1995

THE RSA NEWSLETTER

In This Issue:

Industry leaders back RSA S/MIME plan *Page 1*

Eurocrypt '95 *Page 2*

Time to Change Your Tires *Page 2*

Online Services Call Truce in Web Security War *Page 3*

RSA Announces New Export Consulting Services *Page 4*

New RSA Product Wins Industry Award *Page 5*

RSA Licensee Spotlight: ConnectSoft *Page 6*

5th Annual RSA Conference Selling Out *Page 7*

RSA Spins Off Certificate Services: VeriSign, Inc. is Born *Page 7*

Register NOW for the January RSA Conference!

See page 7 for details.

Lotus, Microsoft, Banyan and other industry leaders back RSA S/MIME plan

Several major networking and messaging vendors, in conjunction with RSA Data Security recently announced their endorsement of a specification for interoperable e-mail security, to be known as "S/MIME", short for "Secure/Multipurpose Internet Mail Extensions." Several of the vendors announced plans to release S/MIME-compliant products this quarter.

The S/MIME specification is based on the popular Internet MIME standard (RFC 1521), which provides a general structure for the content type of Internet mail messages and allows extensions for new content type applications... like security. S/MIME will allow vendors to independently develop interoperable RSA-based security for their e-mail platforms, so that an S/MIME message composed and encrypted on one vendor's application can be successfully received and decrypted on a different one.

Major vendors who announced support forthe S/MIME secure interoperable e-mail plan include Microsoft, Lotus, Banyan, ConnectSoft, QUALCOMM, Frontier Technologies, Network Computing Devices, FTP Software, Wollongong, SecureWare and RSA.

"We fully expect S/MIME to be the defacto standard for vendor-independent email encryption."

Sophisticated encryption and authentication technology has been viewed as the crucial enabling technology for electronic commerce over the World-Wide-Web — but encryption has been slow to come to e-mail, with most packages offering no security whatsoever. "Commercial e-mail packages don't offer encryption because, up until now, there have been few open security specifications," said Jim Bidzos, RSA President. "Internet Privacy-Enhanced Mail (PEM) is excellent for text-based messages. MIME represents then next generation, and has been widely

continued on page 3

Doing Business in a Global Marketplace: Secure Electronic Commerce

by Lew Jenkins, President, Premenos Corporation

Today's higher-bandwidth communications and networking technologies are offering vast potential for secure, integrated EDI in an open, global environment. The term "Electronic Commerce" has become popular recently as growing numbers of corporations are recognizing the huge business potential of open networks.

In fact, EDI and its role in electronic commerce are figuring prominently in discussions about the proposed National Information Infrastructure (NII).

A Department of Commerce publication had this to say about electronic commerce's potential impact on business: "The NII endorses electronic commerce applications because they will help U.S. companies increase productivity by enabling rapid business transactions, data and informa-

continued on page 8

Eurocrypt '95

Eurocrypt '95 was held a few months ago in St. Malo, in Brittany on the northern coast of France. This was the most international Eurocrypt ever, with over 350 participants from countries such as Russia, Rumania, Brazil, South Africa, Bulgaria, Singapore, and the Czech Republic. It was a great conference in a beautiful location (with more wine than you normally see at cryptography conferences).

The 33 papers presented were generally of high quality, although there were no major revelations. From my perspective, the two most clever ideas came from the rump session (Rump sessions are reserved for unique ideas and works in progress. This year, there were 24 talks of 5 minutes each).

The first clever idea is from Adi Shamir, one of the inventors of RSA. In RSA, the modulus is $n = pq$, with public exponent e and private exponent d. Shamir observed that if the receiver knows that the message to be encrypted is smaller than p, then the recipient *only* needs to decrypt *mod p*. In mathematical language, if the plaintext is $x<p$, then the ciphertext is $c = x^e \bmod n$. Decryption is simply $x = c^d \bmod p$.

Shamir's idea applies to especially paranoid users who want to use enormous moduli — 5000 bits, for example. Factoring such a large modulus is impossible with today's technology, but encryption and decryption are slow if p and q are of equal size. However, if p is 500 bits long and q is 4500 bits long, then the best current factoring algorithms — the quadratic sieve and the number field sieve — don't work any faster. But if x is limited to 500 bits, decryption goes very quickly. Since we can always choose a small value for e, encryption is still efficient.

Another obvious application of Shamir's idea is in current implementations with, for instance, p and q of about 256 bits. If RSA is just used for key exchange, then x can almost always be less than 256 bits.

The idea of encrypting *mod p* and *mod q* separately has been around for some years, but as far as I know, Shamir is the first to make this particular observation.

The second clever idea was from Louis Guillou and Jean-Jacques Quisquater, who questioned whether RSA signatures are really longer than DSA signatures. Since an RSA modulus is usually at least 512 bits and DSA signatures are 320 bits, it seems obvious that DSA is shorter.

However, if you use a hash function (SHA, for example), then the actual message signed will only be 160 bits long. This hash would normally be signed using the RSA algorithm, and then appended to the message. The clever idea is to fill up the remainder of the 512 bits with part of the message, rather than wasting it by filling it up with padding. This part of the message is recovered during signature verification. Thus, RSA uses 160 bits plus the message length, while DSA uses 320 bits plus the message length!

For large messages RSA will always be faster than DSA, no matter how long a modulus you use.

Actually, things are not quite this straightforward. For instance, an RSA signature cannot be less than 512 bits, so DSA is faster for very short messages. For large messages, RSA will always win, no matter how long a modulus you use. This is an amazingly clever idea — simple and useful — but one I have never seen before.

If you're interested, the full Eurocrypt '95 conference proceedings are available from Springer-Verlag in their *Lecture Notes for Computer Science series: Advances in Cryptology — Eurocrypt '95*, edited by Louis C. Guillou and Jean-Jacques Quisquater (ISBN 3-540-594-094).

— *Bruce Schneier*
reprinted from Dr. Dobbs's Journal

Mr. Schneier's "Applied Cryptography — Second Edition" will be published by John Wiley & Sons this November.

Time to change your tires...

Part of RSADSI's job is to constantly monitor the state-of-the-art in cryptology and attacks upon RSA-developed cryptosystems. RSA mathematicians anticipate that sometime this year, for the first time ever, a single 512-bit RSA key will be successfully factored (i.e. "cracked") using a team of several thousand workstations scattered across the Internet. This represents an enormous amount of computational effort expended to crack the equivalent of just one person's RSA keypair, and as such does not represent a general "solution" to RSA-encrypted data.

However, whenever a large number is successfully factored, there are certain to be a few uninformed inflammatory reports in the media reporting that "RSA has been broken" or that "RSA is insecure". Of course, while such an accomplishment would be academically impressive, it does not mean that the RSA Public Key Cryptosystem has been "broken"; in fact, RSA remains secure.

As with any cryptosystem, the size of RSA keys should be steadily increased to keep pace with advances in computational power and mathematical theory. To this end, if you use RSA moduli of 512 bits or smaller, you may want to consider increasing the size of your keys. The table below, derived from the RSA Labs report, compares the anticipated strength of 512-bit and 768 bit moduli over the next four years:

Time to factor, with an initial $100,000 investment in computing power		
	512 bits	768 bits
1996	9.5 years	6.3×10^4 yrs
1997	6.0 yrs	4.0×10^4 yrs
1998	3.8 yrs	2.5×10^4 yrs
1999	2.4 yrs	1.8×10^4 yrs

This information is for comparison purposes only, and is based on current factoring technology

Clearly, it behooves you to move to larger keys as soon as is practical. Should you have any questions regarding this or any other issue relating to information security or cryptography, RSA's resources are (as always) at your disposal. Copies of the RSA Labs paper, "The Security of 512-bit RSA" are available at our web site, www.rsa.com, or in printed form directly from RSA Laboratories.

New RSA Licensees

Look for new RSA-secured products from our newest partners! Many of these new licensees will be demonstrating products at the upcoming 1996 RSA Data Security Conference in January.

- Aquila Technologies
- Intuit • Wollongong
- V-ONE Corporation
- Broadvision • ConnectSoft
- Checkpoint Software
- Working Set • software.com
- Internet Factory
- Open Market • Spyglass
- VISA Interactive
- Frontier • Motorola
- IBM (Dynamic DNS)
- NEC (CDPD) • eSHOP
- Interval Systems
- StarNine • CommPress
- Encyclopedia Britannica
- Symantec • Wakefield
- Open Software Foundation
- IBM (CDPD) • Taligent
- Mitsubishi (CDPD)
- Collabra • Transcrypt
- Software Partners

Netscape, Terisa, IBM, AOL, Compuserve & Prodigy Call Truce in Web Security War

Terisa Systems, the joint venture between RSA and EIT, announced last April that itexpects to receive investments and technology from the three leading on-line service providers, plus two Internet technology developers to create a universal approach to Internet security.

A common interoperable approach should make it easier for information providers to provide secure information on the World Wide Web, and easier for consumers to access it. By incorporating the two leading transaction security standards, Secure HTTP (HyperText Transfer Protocol) from Enterprise Integration Technologies and SSL (Secure Sockets Layer) from Netscape into a single development package, Terisa can offer an approach that ensures application interoperability — that is, applications will be able to communicate securely even though they may have been offered by different organizations.

Assurance of secure transactions is required for net-based shopping, the sale of information over the net, and applications that require secure forms as a part of business operations. Pursuant to a letter of intent (LOI) executed on April 6, America Online Inc., CompuServe, IBM, and Netscape Communications intend to become equity holders in Terisa along with Terisa founders Enterprise Integration Technologies andRSA Data Security, Inc. In addition, Prodigy has indicated an intent to become an adopter and implementer of Terisa's technologies. Olivetti will represent Terisa's interests in the European markets.

Terisa plans to introduce a tool kit that combines the two major transaction security protocols in the market today, Secure HTTP and SSL. This will eliminate customer concern about whether the protocols being used to implement security in their applications will work with other applications — full interoperability will be assured.

Terisa's tool kits support the popular RSA public key cryptography and other cryptographic systems. Products developed withthe new tool kits will be compatible with the installed base of Netscape SSL applications. End users should expect to see commercial products based on the new technology by late 1995.

The specifications for the individual security technologies used in the tool kit have already been submitted to the appropriate standards boards, according to Allan Schiffman, Terisa's chief technology officer

continued on page 6

S/MIME *continued from page 1*

adopted because of its ability to handle nearly any content type. The new S/MIME allows you to secure this rich content."

"We fully expect S/MIME to be the defacto standard for vendor-independent e-mail encryption. Solid encryption is something that our customers have been asking us for, but up until now, we didn't have a viable option. S/MIME gives them everything they want: RSA encryption, digital signatures, and the ability to mix different vendors' e-mail systems without losing that security," said Bob Dickinson, ConnectSoft Vice President and General Manager Consumer Online Products & Services Division.

"Frontier Technologies believes that in the future most companies will routinely encrypt electronic mail messages sent over the public Internet," said Dr. Prakash Ambegaonkar, Frontier Technologies' president. "This will only happen once there is a well-understood standard for secure email that is easy to implement. Frontier has several years experience in developing secure email solutions. In order to speed the adoption of the S/MIME specification, Frontier Technologies intends not only to be one of the first vendors to support S/MIME in its networking software, but to also make our initial implementa

continued on page 4

RSA Announces New Export Consulting Services

RSA Data Security is proud to announce a new portfolio of comprehensive export consulting services. These offerings are designed to make it easier for developers to maneuver in Washington's bureaucratic export licensing maze.

Renee Danckwerth, head of RSA's Export Consulting Services

Heading up RSA's new export services office in Annapolis, Maryland, is Renee Danckwerth. Ms. Danckwerth has extensive experience in the fields of export licensing and defense trade control, and in fact worked in those offices at DoD and National Security Agency for several years. Ms. Danckwerth holds the unique dual advantages of knowing the system and knowing the people personally involved at every step of the export licensing process, and as such, is uniquely qualified to fast-track your product and export paperwork.

Brief overviews of RSA's new export services are listed below; for information on pricing and availability, contact your RSA representative.

HALF-DAY GENERAL EXPORT BRIEFING

This presentation provides an introduction to the who, what, how, and why of U.S. Government encryption export controls. RSA's experienced Washington-based export consultants explain the relevant agencies and regulations, and demonstrate how they apply to your company and products:

- Develop a better understanding of the Government's export policy to maximize your participation in foreign markets.
- Hear an insider's perspective on the export licensing procedure and product evaluation processes.
- Learn how to compose your own Corporate Export Plan.
- Receive essential export forms and documentation.
- Obtain reliable, informed answers to your export questions.

PRODUCT EXPORT ASSESSMENT

RSA's export consultants will thoroughly review your finished product and report on the probable impact of relevant government encryption export regulations. The report will detail all applicable export regulations, suggest possible modifications you might make to the product that could expand your access to foreign markets and ease export licensing procedures, and outline your best approach to filing for export licenses. (Please allow two weeks for completion of the assessment and delivery of your report).

EXPORT LICENSING ASSISTANCE

The US Department of State receives a few hundred commodity jurisdiction requests, over one thousand agreements, and tens of thousands license applications each year. The slightest discrepancy can create serious delays on the already lengthy export license processing times. RSA's export specialists know the procedure and the paperwork. Let us handle it for you.

PRE-DEVELOPMENT PRODUCT EXPORT LIAISON SERVICES

Our consultants will advise you on crucial decisions like algorithm and keysize selection that can significantly impact your export licensing efforts. In addition, we'll act as a liaison between your development team and government agencies so that when your product is ready to go, so is your export license. Status reports would be provided on a monthly basis. (Timeframe for these services vary; 50-75 hours over a 3 month period is typical).

For more information about RSA's export related services, contact your RSA representative.

S/MIME *continued from page 3*

tion of the S/MIME protocol freely available for other vendors to use as a reference."

"The freedom to have a private conversation is fundamental to personal communication that is the essence of electronic mail," said John Noerenberg, Director of Engineering for QUEST products at QUALCOMM. "Wide-spread acceptance of specs like S/MIME make it possible for individuals and organizations alike to conduct their business over the net secure in the knowledge that their private business is, in fact, private."

"FTP Software is glad to endorse the S/MIME blueprint for secure electronic communication," said John O'Hara, director of development for FTP Software. "Whether communicating with customers, business partners or remote offices, companies need to ensure that confidential information stays confidential. This was difficult in the past, since organizations are connected through diverse messaging systems from competing vendors. S/MIME eliminates those barriers by facilitating implementations across multiple vendor products."

S/MIME is based on the intervendor PKCS (Public Key Cryptography Standards) which were established by a consortium of RSA, Microsoft, Lotus, Apple, Novell, Digital, Sun and the Massachusetts Institute of Technology in 1991. PKCS is the most widely implemented suite of commercial cryptographic standards in the United States. The common PKCS specifications allow developers to independently develop secure applications that will interoperate with other PKCS-secured applications.

Developers interested in S/MIME can get more information at RSA's web site, in the "What's New" section at http://www.rsa.com.

New RSA Product Wins Industry Award

"Key Escrow Done Right" — Wired Magazine

RSA Secure, RSA's newest enterprise encryption product has been named "Best Encryption Product" in the coveted Infosecurity News Readers Trust Awards in a ceremony in Washington D.C. last June.

RSA Secure won the award in a hotly contested category, beating products including AT&T's Secret Agent and Viacrypt's PGP.

INFO SECURITY NEWS
READERS TRUST AWARD
Winner

With RSA Secure, users can encrypt a single file — or anentire hard disk — with a few mouse clicks. RSA Secure is designed to be the easiest, most secure way to protect sensitive information on a PC, Mac or Sun. The software, which provides facilities for self-escrow of encryption keys, provides a user-controlled alternative to thegovernment's proposed federally-basedescrow system, popularly known as the "Clipper".

DESIGNED SPECIFICALLY TO FOIL HACKERS — With the recent rash of serious attacks on computer networks by hackers, private and corporate computer users are looking for ways to protect themselves. RSA Secure can provide a big part of the solution — because even if an attacker successfully gains access to your network or workstation, they won't be able to read any of the files they might steal. RSA Secure's encryption provides the final line of defense against hackers by encrypting files with RSA's own powerful RC4 Symmetric Stream Cipher, which is orders of magnitude more secure than the government's DES encryption standard.

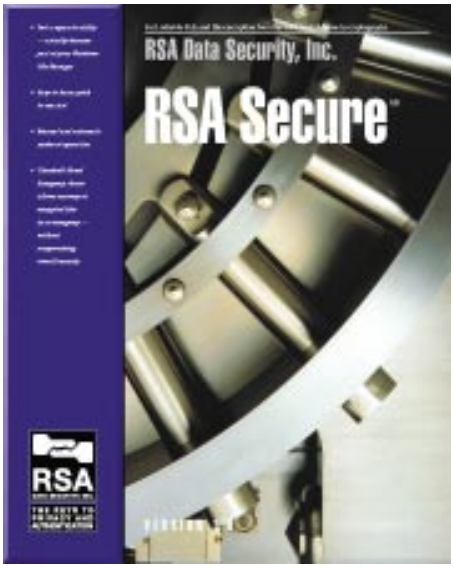
Laptop owners need to protect the valuable corporate databases and contact lists that they travel with. If the laptop is lost or stolen, that confidential data is gone, too — and is most likely in someone else's hands. RSA Secure can make even the most sensitive data carried on laptops useless towould-be thieves. On the other hand, users attached to a network need to guard electronic threats: hackers and intra-company snooping. Even if a user isn't confident about the security of their network, they can still provide for the protection of their own files with RSA Secure. Hackers or crooked insiders lurking the network will be unable to read RSA-secured files.

PERSONAL, NOT GOVERNMENT, KEY ESCROW — In emergency situations where a user is unavailable, employers sometimes must have access to that user's encrypted files. To address these cases, most disk-locking applications on the market use simplistic "skeleton key" systems to allow system administrators access. But that is an invitation to abuse. One crooked insider can compromise an entire network. Only RSA Secure features Threshold Based Emergency Access™. Using the patented RSA Public Key Cryptosystem™ along with RSA's advanced key storage and secret sharing technologies, RSA Secure allows administrators to split that emergency decryption authority among up to 256 different trustees, some subset of which must concur in order to decrypt a user's files. Administrators further determine the threshold number (say, "any 3 out of 5" predetermined trustees) that must concur (by inserting their escrow key disks) in order to decrypt a user's personal files in an emergency. No other product on the market offers such advanced privacy guards or such sophisticated escrow capabilities.

NOT A SEPARATE UTILITY — RSA Secure is designed for users of PC's, Macs or Suns that are attached to a network or stand-alone or remote. The program is not a separate utility — it actually embeds itself into the file system native to each platform. For example, when installing on a Windows PC, RSA Secure actually becomes part of the Windows File Manager subsystem, adding a new "RSA" menu item in the File Manager menu bar.

AUTOMATIC OR MANUAL ENCRYPTION — With the AutoCrypt™ feature, users can define sets of files and directories that are automatically encrypted and decrypted (for example, every time a user goes in or out of Windows). Individual files or sets of directories can be encrypted quickly and easily, and users can encrypt files anywhere, not just in special "secured directories." Passwords can be changed at any time, without decrypting all files previously encrypted under another password (a big advantage over other encryption utilities).

FAST ENCRYPTION + RSA SECURITY — In the security business, RSA is synonymous with encryption. For bulk file encryption, RSA Secure uses our fastest, most secure stream cipher: the RC4™ Symmetric Stream Cipher. The RC4 cipher is already a standard in many high-speed encryption



applications, such as Cellular Digital Packet Data (CDPD) devices and software, and is also used in products like Microsoft Windows NT, Windows for Workgroups and Apple MacOS 7.5. This implementation, which uses 80-bit RC4 keys, provides many, many orders of magnitude more security than the government's DES encryption system. The high speed of RC4 allows RSA Secure to achieve throughputs of over 850,000 bps on a typical 486/33mhz, even when the complex Emergency Access key escrowing features are activated.

For more information about RSA Secure, contact Product Manager Dana Ellingen at RSA.

RSA Licensee Spotlight: ConnectSoft

ConnectSoft, Inc., providers of the most powerful, easy-to-use interfaces to digital communication and commerce, announced recently that it has licensed a new interoperable security technology from RSA that will provide ConnectSoft customers with added privacy and security to their daily communications. The agreement will allow ConnectSoft to make products that comply with the S/MIME (Secure Multipurpose Internet Mail Extensions) specification. S/MIME willensure that a customer's e-mail is read only by the designated recipient — regardless of the e-mail platform they're using. The new security features will be included in the newest versions of ConnectSoft's E-Mail Connection and Internet Connection products that will be released this fall.

"In today's networked world, security is a growing concern as we rely on e-mail for more of our day-to-day communications," said Bob Dickinson, ConnectSoft's vice president and general manager, Consumer Online Products & Services division.

"Our arrangement with RSA provides encryption and authentication technologies giving our customers the most protected and secure communication available today."

GLOBAL SECURITY STANDARD

Encryption and authentication have been viewed as crucial enabling technologies for electronic commerce of the World-Wide-Web — but encryption has been slow to come to e-mail, with most packages offering nothing at all. "ConnectSoft's early support of S/MIME demonstrates its commitment to provide customers with secure digital communication as well as its sophistication in developing future electronic commerce solutions," said Jim Bidzos, RSA president.

"If one public-key system is used everywhere for authentication, then signed digital documents can be exchanged between users in different countries using different software on different platforms. This interoperability is necessary for a true digital economy to develop," Bidzos said.

ConnectSoft is a privately held company based in Bellevue, Wash. The Consumer Online Products division markets the company's award winning products, such as E-Mail Connection, Internet Connection and KidMail Connection. The Commercial Software Development Services division develops custom software which enables secure, digital communications, commercial transactions, and Integrated Logistics Systems for Fortune 1000 companies such as United Parcel Service (UPS). The recently formed Commercial Network Services division will provide high-bandwidth, high-quality commercial Internet and TCP/IP services to large and medium sized companies throughout the United States.

For more information, contact ConnectSoft at 206/827-6467.

WWW Security War Truce *continued from page 3*

and designer of S-HTTP. "We plan to work closely with groups such as the World Wide Web Consortium and the Internet Engineering Task Force to unify these two approaches to make it easier for developers and end users to facilitate secure transactions on the Web," he said.

Terisa plans to recruit an advisory board of industry experts to assist in defining strategies and technology to achieve its goalof continuing to develop commercially viable transaction security.

"Despite the growing interest in the Internet, the commercial potential has been held back by competing and incompatible security approaches," said Steve Case, president and CEO of America Online, Inc. "What the market needs is a unified, interoperable approach to security that is widely embraced. We are pleased to be part of this industry standards-building effort, as we believe it represents a critical step on the path to building a mass market for interactive services."

Tim Oren, CompuServe vice president of future technology, concurred, adding "We all recognize that expanded electronic commerce requires a stable security base. This must be coupled with innovative solutions that cover a broad range of security issues and address differences between various types of transactions. The Terisa partnership is a major step toward a unified security solution that will enable the global information infrastructure to achieve its fullpotential."

"Open standards for security on the World Wide Web become more important every day," said John Patrick, IBM vice president of Internet applications. "Terisa helps all of us meet the needs of customers who want universal security approaches for the Web — it's a cooperative approach that dovetails well with IBM's overall strategy."

"Netscape has already announced we will be supporting both SSL and S-HTTP in our products to provide maximum interoperability for our customers. Our partnership with Terisa provides a further channel for ensuring orderly development of much-needed security approaches for the Internet," said Marc Andreessen, Netscape vice president of technology.

Terisa plans to make low cost licensing of its technology broadly available to developers. For widespread acceptance of electronic transaction security, users must have both confidence in the technology and a minimum of implementation difficulty. Terisa's SecureWeb™ tool kits are available for Microsoft Windows and Macintosh environments, and all popular UNIX platforms including Sun, HP, IBM, Silicon Graphics, and Digital systems.

5th Annual RSA Conference Selling Out

JANUARY 17-19, 1996, FAIRMONT HOTEL, SAN FRANCISCO

First held in 1991, RSA's annual conference is today considered the industry's premier cryptography summit. More than 1,000 participants are expected to attend the 1996 conference, which has outgrown its Redwood City roots and will now be held at the historic Fairmont Hotel atop Nob Hill in San Francisco.

"The RSA conference is a must for anyone involved with cryptography, electronic commerce, or any Internet application," said Jim Bidzos, president. "It is an opportunity for business people, leading academic cryptographers, and representatives of government to gather and debate the technology and business issues facing this industry.

"This conference is where trends are set and where standards become products, making it especially valuable for industry watchers in the media and analyst communities."

The program will focus on the commercial applications of modern cryptographic technology, with an emphasis on Public Key Cryptosystems. There will be presentations and products from RSA's major licensees, including Microsoft, Visa, Intuit, Apple, Novell, Lotus and many others. Panel discussions will cover topics such as CLIPPER, FORTEZZA and key escrow. Tutorials will range from the basics of crypto theory to cutting-edge applications.

For more information and to register, contact RSA's conference organizer, Layne Kaplan Events, at (415) 340-9300. Registration is $395 until November 17th, and thereafter $495. Late registration (after December 31st) is $695, on a space-available basis. Register early — the RSA Conference is always a sell-out!

RSA spins off Certificate Services: VeriSign, Inc. is Born

Network and Information Superhighway users can now trust the contents of an electronic transmission and the identity ofits source with the recent launch of VeriSign, Inc.

The new company, which germinated from the seed of RSA's Certificate Services division, is positioning itself as the first full-service provider of Digital ID's, also known as X.509 digital certificates. Digital IDs ensure privacy and authenticate the content of electronic transmissions on all public and private networks.

VeriSign was formed with the financial backing of a diverse group of industry leaders including Ameritech, Bessemer Venture Partners, Fischer International, Mitsubishi, RSA Data Security, Security Dynamics, and Visa International.

"The growth of electronic commerce and the growing commercial use of the Internet have heightened the need for secure and trusted communications," said Richard Madrid, Product Director of Electronic Commerce, Ameritech Corp. "We are investing in VeriSign to help create products that will deliver a trusted and secure transaction environment."

"Advances in data processing and communications have increased the need for servicing new forms of digital identity which VeriSign is uniquely positioned to provide," said Bill Powar, Visa International Vice President. "Visa's mission is to represent the interest of our Member financial institutions in the introduction and development of new technologies and this investment will ensure that Member needs are addressed as this market evolves."

"You may think that encryption equals total security, but it merely ensures that others can't read your data," explained Jim Bidzos, VeriSign founder and Chairman ofthe Board, and President of RSA Data Security, Inc. "You don't really know who sent an encrypted document. Just because someone has a password or an e-mail address, doesn't mean you can trust that they are who they say they are. A Digital ID assures you that the data was sent by the right person and that the contents haven't been altered on the way."

Current Digital ID-enabled products from Apple Computer and Netscape Communications demonstrate the rapidly evolving industry support for such technologies. Digital IDs are quickly becoming an essential component for secure global electronic transactions.

"VeriSign is the only real Digital ID issuing company in the world," said Yoshito Nakamura, Assistant General Manager Technology Affairs Department, Mitsubishi Corp. "We invested in VeriSign because we see this technology as critical to developing trust over electronic commerce. Our global trading business is moving towards electronic commerce, and we see VeriSign's ability to provide Digital IDs strategic to our future global trading business."

"The certification services performed by VeriSign should facilitate growth in electronic commerce, messaging and corporate networking applications requiring a high degree of data privacy and integrity, and sender non-repudiation," said Charles Stuckey, President and CEO, Security Dynamics.

VeriSign's Independent Software Vendor (ISV) partners will add Digital ID capabilities to their cryptography-enabled applications, ensuring the privacy and authentication of electronic documents, electronic commerce and e-mail.

VeriSign now offers end users Digital ID certification services and provides a consistent identification framework. VeriSign issues Digital IDs which certify the individual identity of a public key holder. The person can then use any VeriSign enabled applications to send VeriSigned documents and transactions. VeriSign will also license other companies to provide this service.

For more information, contact VeriSign at (415)508-1151.

 continued from page 1

tion exchanges and organization changes. [With these applications] organizations can re-engineer their business processes. The immediate effect will be to enhance the performance of the U.S. economy."

NEW ELECTRONIC COMMERCE REQUIREMENTS

As open communications technologies continue to mature, companies are setting new expectations for their electronic commerce applications. If they are traditional EDI users, they require the ability to extend andenhance their existing EDI infrastructures to take advantage of open networks. At the same time, many are adopting a corporate information infrastructure based on client/server architecture — requiring EDI solutions that are compatible with thenew environment. Finally, companies are requiring built-in, end-to-end security for their electronic commerce transactions, and they're expecting the levels of speed and easy routing that TCP/IP and IP networks provide.

National information initiatives call for networks that will enable "meta mail," or secure messaging applications that are notdependent on the transport mechanism. These proposed networks will facilitate next generation, integrated EDI featuring built-in security based on the RSA encryption algorithm, and robust routing by content type.

A STRATEGY FOR OPEN ELECTRONIC COMMERCE

The ideal solution, or "family of products," will enable all electronic commerce applications to occur over a variety of public and private communications networks. Companies have made significant investments in their current communications infrastructures and systems. Therefore, electronic commerce products must enhance existing EDI and communications networks in the following ways:

- Reduce the cost — regardless of volume — of doing business electronically by a significant amount (no published numbers yet).
- Provide secure, reliable end-to-end business applications over any network offering, public or private.
- Provide an open, scalable, and standards-based solution that grows with a company's business.
- Offer the necessary service and support that is key to any business process.
- Continue to work with VANs, VASP, and other existing service providers.

The vision that successful electronic commerce will build upon is the well-established reputation of EDI transactions and practices to provide electronic commerce solutions for open networks such as the Internet and other IP services.

Ultimately, this vision will allow an open architecture where products and technology allow companies to extend the existing model of EDI to further provide secure, cost-effective business electronically in a global marketplace.

RSA DATA SECURITY, INC.
100 MARINE PARKWAY
SUITE 500
REDWOOD CITY
CA 94065-1031

FIRST CLASS MAIL
ZIP + 4 PRESORT
U.S. POSTAGE PAID
MMS, INC.

A publication of RSA Data Security, Inc. Copyright © 1995 RSA Data Security, Inc. All rights reserved. For reprints, call your RSA representative.