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

Ciphertext
THE RSA NEWSLETTER

Volume 4, No. 1 Spring 1996

In This Issue:

RSA Conference Draws Record Crowds *Page 1*

RSA Establishes New Pacific Rim Ventures *Page 1*

LOCT: RSA's Next Generation Architecture for Secure Applications *Page 2*

RSA Laboratories Publishes New Security Bulletins *Page 3*

New "Genuine RSA" Branding Program for Secure Products *Page 3*

RSA S/WAN Initiative Champions Proposed IETF IPSec Standard *Page 4*

RSA Place Schedule of Events *Page 4*

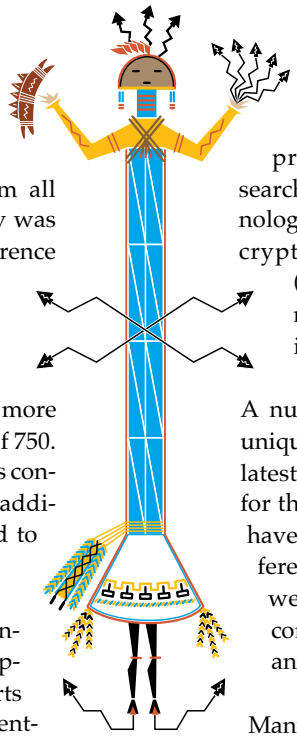
RSA Releases BSAFE 3.0 *Page 5*

RSA Supports SET Standard for Secure Payments over the Internet *Page 6*

MedPlus & RSA Team Up to Save Healthcare Costs and Lives *Page 6*

Visit RSA's Online Art Gallery *Page 7*

RSA Conference Draws Record Crowds



The 5th annual RSA Data Security conference was held January 17-19, firmly establishing its reputation as the industry's foremost cryptography summit. Turnout from all areas of the crypto community was overwhelming, and sent conference organizers scrambling to accommodate a rush of last minute registrants. This fifth annual conference attracted an audience of 1,200 — nearly 40% more than the expected attendance of 750. Despite the best efforts of RSA's conference staff, more than 200 additional unregistered people had to be turned away at the door.

This year's conference drew hundreds of mathematicians, cryptographers and security experts from around the world, representing the best and the brightest of the international cryptographic community. Some attendees came to catch up on the latest developments in data security straight from the industry's leading minds. Others came to share the progress of their ongoing research or to reveal entirely new technologies and applications. Many of cryptography's most recognized (and soon to be recognized) names made a point of attending the conference todo both.

A number of companies used this unique occasion to announce their latest products and developments for the coming year. If you did not have the chance to attend the conference, you should visit the RSA web site (*http://www.rsa.com*) for complete details of many of these announcements.

Many products and initiatives were officially announced at the conference, such as Digital's speedy new Alpha encryp-

continued on back page

RSA Establishes New Pacific Rim Ventures: Agreements with China and Japan

Global Cryptography: those were the watchwords of the latest RSA Conference, as evidenced by RSA's recent announcements of partnerships with organizations in Japan and the People's Republic of China.

Headquartered in Tokyo, Nihon RSA will provide developers in Japan with access toRSA's full suite of encryption technology, including RSA's BSAFE and TIPEM toolkits. This is the identical technology previously licensed to Microsoft, IBM, Netscape, Intuit, and others. Nihon RSA will market a local version of RSA's award-winning RSA Secure™ product, which enables Windows and Mac users to easily, quickly and securely encrypt their hard drives.

continued on page 3

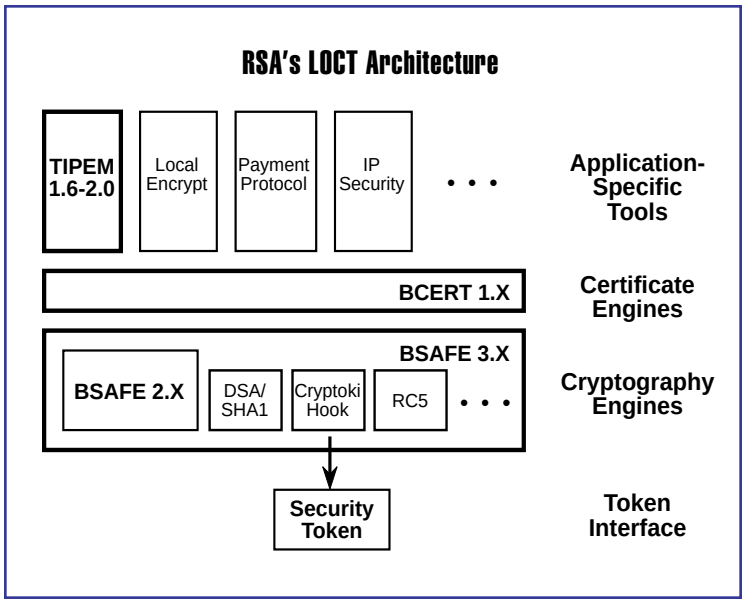
RSA Data Security Reveals Next-Generation Architecture Strategy for Building Secure Applications

RSA Data Security, Inc. unveiled its strategic vision in the form of a next-generation architecture, the Layered Open Crypto Toolkit (LOCT™). Destined to be a road map for future security solutions from RSA and its vendor partners, the LOCT architecture outlines a framework for cryptographic security applications, application programming interfaces (APIs) and tools.

Unveiled at the 1996 RSA Data Security Conference, LOCT provides developers with a more open, extensible and flexible environment that enhances security and ease of use. The introduction of the LOCT architecture is underscored by the simultaneous announcement of BSAFE 3.0, the latest version of RSA's industry-leading cryptography engine for software developers. BSAFE, which forms the foundation of RSA's security vision, now includes significant security enhancements and performance improvements, as well as support for additional standards.

"With the explosion of remote computing, corporations are very concerned about building security into their applications," said Jim Bidzos, president of RSA. "With RSA's next-generation LOCT architecture, which raises the bar for security standards, there is finally an open, systematic method for building reliable security solutions."

More than 80 new OEM partners have joined RSA in the past year, including Intel, Lotus, Microsoft and IBM. Now, more than 200 RSA partners — more than any other security solutions provider — are making RSA-enabled products available to companies around the globe. With the introduction of LOCT, RSA expects that even more partners will join with the company to deliver state-of-the-art security solutions to the world's corporations.



RSA's LOCT architecture comprises four layers including: application-specific tools, token interface, cryptography engine, and certificate engine. LOCT's layered architecture, which reduces redundancy in separate toolkits and applications, enables developers to build crypto applications with lower overhead, smaller code size and decreased memory requirements. In addition, the published API is more open, allowing any vendor to write application-specific tools that interface to LOCT's certificate and cryptography engine layers.

LOCT provides developers with a more open, extensible and flexible environment that enhances security and ease of use.

The application-specific tools layer of LOCT provides developers with cryptography protocols and standards that work with existing embedded applications, such as S/MIME, virtual private networks (VPNs) or electronic data interchange (EDI). Using this LOCT layer, developers can expect to save substantial development time and create better results, since they are shielded from the "guts" of the cryptography and can avoid common programming mistakes.

RSA's token interface layer, which provides compatibility with any security token or card that is compliant with the Cryptographic Token Interface (Cryptoki), allows application developers to immediately take advantage of new tokens from different vendors — without writing or embedding custom interface code. Cryptoki is an interoperability specification developed by RSA and supported by virtually the entire security-token industry.

For simplified support, as well as update and export considerations, LOCT's cryptography engine layer provides all encryption and authentication services. This includes a centralized trusted crypto resource, which provides access to proven and tested algorithms, as well as the most efficient implementations.

Finally, the certificate engine layer of RSA's LOCT architecture enables standardized and centralized X.509 public key certificate management functions. This capability providesdevelopers with a generic certificate services layer that can interface with any cryptography engine or application-specific tool or application. This layer is independent of applications or messaging formats.

"VeriSign is excited to be working with RSA to enable and promote the new LOCT architecture," said Stratton Sclavos, president and CEO of VeriSign. "Developers looking to build public-key enabled solutions can utilize the new architecture and VeriSign's solutions for the LOCT certificate management layer to rapidly deploy secure electronic commerce solutions."

For more information on LOCT and RSA products employing the LOCT architecture, contact RSA at *http://www.rsa.com*.

RSA Laboratories Publishes New Security Bulletins

RSA Laboratories introduces a new publication for 1996: the RSA Laboratories *Bulletin*. RSA Labs is the mathematics research and development arm of RSA, and is charged with reviewing, designing and implementing secure and efficient cryptosystems of all kinds. The *Bulletin* is a short, periodic newsletter designed to update developers on the latest threats and attacks to various cryptosystems, as well as educate them on common development oversights and mistakes that can cripple otherwise safe cryptosystems. More than just "cursing the darkness", the *Bulletin* will also "light a candle" by striving to provide solutions and preventative measures to the coomon problems that face the developer tasked with providing security for the application.

Each Bulletin is written to address a specific threat or common development mistake, explaining how it might make a crypto implementation more vulnerable to attack and how to prevent exposure to this vulnerability. The three issues published to date are, respectively, Suggestions for Random Number Generation in Software, Timing Attacks on Cryptosystems, and Proper Initialization for the BSAFE Random Number Generator. One more Bulletin is expected in March, and will be entitled Hash Function Recommendations.

For more information on RSA Laboratories' Bulletins or regarding any recent developments in cryptography, contact RSA Laboratories at *rsa-labs@rsa.com* or via the Web at *http://www.rsa.com/rsalabs*. To subscribe to the Bulletins, contact your RSA representative.

New "Genuine RSA" Branding Program Creates Seal of Assurance for Consumers

RSA Data Security, Inc., the world's brand name for cryptography, announced its new branding campaign at the company's fifth annual data security conference in San Francisco last month.

The "Genuine RSA Encryption Engine" logo is designed to identify software and hardware products featuring RSA's powerful cryptography technology. The symbol is the first of its kind in the security industry, and acknowledges RSA's position as the worldwide standard for encryption technologies and tools.

"RSA is the de-facto worldwide standard for security," said Jim Bidzos, president ofRSA. "By developing a Genuine RSA brand, we can provide consumers with the assurance that they are buying a product that incorporates state-of-the-art security technology. And, in addition, our new branding program enables our many partner companies to leverage the RSA name and reputation to differentiate their products."

"We're excited about displaying the Genuine RSA logo on our product packaging," said Mike Homer, vice president of Netscape Communications. "The RSA logo shows our customers that we really care about data security, and that they can be confident that Netscape products are protected by the most trusted name in cryptography."

"We use RSA technology in our software," said Kathy Kincaid, director of I/T Security Programs for IBM. "Displaying the Genuine RSA logo will help us stand out from the crowd. The combination of IBM and RSA enables us to deliver the ultimate in cryptography."

RSA's new Genuine RSA Encryption Engine logo can be downloaded from RSA's "ArtGallery" at: *http://www.rsa.com.*

Pacific Rim Ventures

Continued from front page

James Bidzos, RSA's president and chief executive officer, will serve as chairman of Nihon RSA.

"The market in Japan is evolving quickly and the demand for RSA technology is very strong," said Bidzos. "A number of major players in Japan, including companies such as NTT and others, are ready to work with us to make Nihon RSA a success. We also have a long list of prospects seeking to do business with the new subsidiary and license its software, patents and trademarks. Global commerce is a reality today, and Nihon RSA will help further its growth."

RSA Data Security, Inc. will assign its Japanese customers to Nihon RSA. This move will provide the new entity with an immediate royalty revenue stream. Local staff and management are currently under recruitment for the new organization. In addition, RSA and its consultant, Asian Pacific Ventures Co. of Menlo Park, Calif., will invite a limited number of Japanese companies to become investors.

RSA's toolkits have already been exported under license from the US Department of State to NTT, Mitsubishi, BUG, and other companies in Japan. These toolkits offer full-featured RSA technology and are not limited to the usual 40-bit key length restrictions imposed on exported products. "We have been successful in exporting our

continued on page 7

RSA S/WAN Initiative Champions Proposed IETF IPSec Standard

Leading firewall and TCP/IP stack vendors are joining RSA Data Security in bringing the Internet Engineering Task Force's (IETF) proposed "IPSec" security standard several steps closer to realization. The initiative, called S/WAN, designates specifications for implementing IPSec to ensure interoperability among firewall and TCP/IP products.

S/WAN ENABLED
RSA IPSec INTEROPERABILITY FORUM

S/WAN's goal is to use IPSec to allow companies to mix-and-match the best firewall and TCP/IP stack products to build Internet-based Virtual Private Networks (VPNs). Currently, users and administrators are often locked in to single-vendor solutions network-wide, because vendors have been unable to agree upon the details of IPSec implementation. The S/WAN effort should remove a major obstacle to the widespread deployment of secure VPNs.

A number of leading vendors are part of theRSA consortium to finalize S/WAN; including: Bay Networks; CheckPoint Software Technologies, Ltd.; Digital Pathways; Frontier Technologies; FTP Software; Gemini Computers, Inc.; IBM Corporation; Netrend Corporation; Raptor Systems, Inc.; Secure Computing Corporation; Sun Microsystems; TGV Inc.; TimeStep Corporation; Trusted Information Systems, Inc.; V-ONE; VeriSign, Inc.; VPNet; and Attachmate/Wollongong.

RSA is hosting a real-time S/WAN interoperability test — check out the S/WAN page at RSA's website, http://www.rsa.com.

Several of the firewall and stack vendors currently working with RSA plan to announce products in the first quarter of 1996 that support the new S/WAN specification. Many of these vendors assembled at the December IETF meeting in Dallas to test the interoperability of various pilot S/WAN implementations. When testing is complete, sometime early in 1996, the consortium will submit the resulting Implementation Guidelines to the IETF for consideration for inclusion in the IPSec standards.

"VPNs are a low-cost, flexible alternative to private networks," said Jim Bidzos, president of RSA. "However, prior to S/WAN, they were difficult to build and secure, especially since there has been no interoperability across firewalls and secure TCP/IP stacks from different vendors that support data encryption at the IP level. With multiple vendors' support of S/WAN, however, users and network administrators will be free to select the best firewall and stack tools for each part of the network. As a result, we expect companies to implement VPNs in record numbers."

S/WAN is based on the IETF's Security Architecture for the Internet Protocol, RFC 1825-1829, commonly known as "IPSec." S/WAN supports encryption at the IP level, which provides more fundamental, lower-level security than higher-level protocols, such as Secure Socket Layer (SSL) and Secure Hyper-text Transfer Protocol (S/HTTP). RSA engineers expect, however, that higher-level security specifications, including SSL and S/HTTP, will be routinely layered on top of S/WAN implementations, and these security specifications will work together synergistically.

To guarantee IPSec interoperability S/WAN defines a common set of algorithms, modes and options. In addition, S/WAN uses RSA's most advanced block encryption cipher, RC5 Symmetric Block Cipher, which was invented by encryption pioneer Dr. Ron Rivest. S/WAN uses RC5 at key sizes ranging from 40 bits for exportability to 128 bits which can withstand trillions of MIPS-years of computer attack. S/WAN canalso be implemented using the government's older DES algorithm.

RSA PLACE
The premier address for security

RSA is really getting around! Check our schedule below of RSA Place tradeshow appearances and talks by RSA's best-and-brightest. Call RSA Marketing for details on any of these dates.

April 2-4
NETWORLD+INTEROP
Las Vegas

April 25
RSA Day in Washington, D.C.
Renaissance Hotel

April 28-May 1
Electronic Messaging Association
Anaheim

May 1
Internet World (talk)
Santa Clara Mariott

May 20
Internet Security Conference (talk)
London

May 14, 15, 16
CardTech-SecureTech
Atlanta

May 30
Linking Databases to the Internet (talk)
San Francisco

June 4
AFCEA (talk)
Washington DC

June 10-12
6th World Congress of Electronic Commerce
Vancouver

June 12-14
Email World & Internet Expo
Chicago

September 16-20
NETWORLD+INTEROP
Atlanta

Nov 11-13
Computer Security Institute
Chicago

Nov 18-22
COMDEX
Las Vegas

RSA Releases BSAFE™ 3.0: World's Most Popular Cryptography Engine Becomes Faster, Even More Secure

RSA Data Security solidified its leadership position in the cryptography market with its announcement of BSAFE 3.0. Unveiled at the 1996 RSA Data Security Conference, BSAFE 3.0 is the latest version of the company's industry-leading cryptography engine for software developers.

This new version of BSAFE, which underwent nearly a year of testing, includes significant security enhancements and performance improvements, as well as support for additional standards. Now, developers can integrate state-of-the-art privacy and authentication features into virtually any application more easily and rapidly than before. As a result, companies can expect to dramatically reduce the time and costs associated with developing secure applications.

BSAFE 3.0 is the first product built around RSA's new next-generation Layered Open Crypto Toolkit (LOCT) architecture (see article on page 2). This architecture, also announced at the conference, comprises four layers including: application-specific tools, token interface, cryptography engine, and certificate engine.

"In today's environment, security is no longer an option, it's a critical business charter," said Jim Bidzos, president of RSA. "In 1995, RSA signed up more than 80 new licensees, demonstrating that companies are taking this issue very seriously. We expect the worldwide demand for secure applications and networks to continue to grow." Leading manufacturers worldwide have used the BSAFE cryptography toolkit to incorporate RSA encryption technology into more than 200 products, including Novell Netware, Netscape Navigator, Lotus Notes, Digital Internet Tunnel, Oracle SQL*Net, Microsoft Windows 95, and many more.

RSA's next-generation BSAFE engine provides software developers with multiple algorithms and modules for adding encryption and authentication features to any application. BSAFE includes modules for popular encryption techniques, such as RSA, DES, Diffie-Hellman, RC2, and RC4, and also supports improved routines for pseudorandom number generation, as well as digital signatures and certificates.

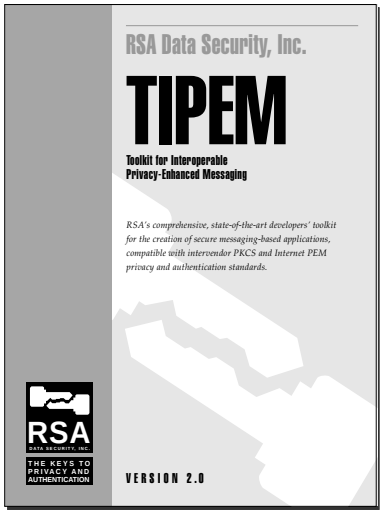
BSAFE 3.0 now supports the high-performance RC5 algorithm, which means that developers can implement secure high bandwidth applications — such as secure video — without resorting to expensive special-purpose crypto hardware. BSAFE also supports a host of government algorithms, including the National Institute of Standards and Technology's (NIST) Digital Signature Algorithm (DSA), the amended Secure Hash Algorithm (SHA1), and a combination of the SHA1 and RSA Digital Signature.

BSAFE also features a unified API for RSA and DSA, making it easier for developers to build solutions for mixed government/commercial crypto environments. In addition, key sizes of up to 2048 bits are allowed for RSA, Diffie-Hellman and DSA algorithms, providing even greater protection.

Several state-of-the-art performance improvements have been made to BSAFE 3.0, including public-key and symmetric-key algorithm enhancements. Plus, dramatic RSA improvements in throughput from four-fold to sixteen-fold are possible, depending on the platform. Performance has also been enhanced for the MD5, DES, RC2, RC4, DESX, DES EDE, and MAC algorithms.

With the introduction of built-in "blinding," BSAFE 3.0 is immune to recently publicized timing attacks on public keys and, as a result, is the only toolkit on the market today to provide this edge. In addition, BSAFE can automatically detect weak keys for DES and other algorithms, providing another level of protection.

RSA also announced TIPEM 2.0, an enhanced toolkit for interoperable privacy-enhanced messaging that facilitates development of secure e-mail and other messaging applications. TIPEM 2.0's unified API simplifies implementation of authentication via RSA Digital Signatures, encryption using RSA Digital Envelopes, and certificate-based key management.



TIPEM 2.0 will be available in the second quarter of 1996, and will support CCITT X.509 V1 and V3 Certificates, PKCS, PEM message formats, and also complies with the new S/MIME specification. It also features an expanded algorithm palette, allowing for support of SHA1, RC5, and Triple-DES.

For more information on upgrading to BSAFE 3.0 or TIPEM 2.0, contact your RSA representative at 415/595-8782.

RSA Announces Support for VISA/MasterCard SET Standard for Secure Payments Over the Internet

RSA Data Security will provide solutions in support of Secure Electronic Transactions (SET), the new technical standard that will enable secure bankcard transactions over the Internet.

The first of such offerings, which allow developers to build SET-compliant applications, is available now as a free upgrade module for RSA's industry-leading BSAFE 3.0 encryption engine. Later this year, RSA will release a "SET-specific" toolkit for developers.

The SET standard, developed jointly by MasterCard International, Visa International and other companies, is based on RSA's widely accepted Public Key Cryptography Standards, specifically the PKCS #7 secure messaging standard. PKCS was originally designed to foster interoperability among vendors using RSA technology. RSA and a consortium of influential partners, including Microsoft, Lotus, Sun, M.I.T. and others, developed the standards in 1991.

"The publishing of the new SET standard represents one of the most important milestones in the evolution of secure electronic commerce over the Internet," said Jim Bidzos, president and CEO of RSA. "Now, developers can easily create new credit-card payment applications for the Internet. We're pleased to be part of this industry effort."

Bidzos added that RSA provided cryptographic expertise and oversight to MasterCard and VISA developers in order to ensure that the SET specification offers the highest quality, as well as the most efficient and secure RSA cryptographic technology possible.

RSA plans to provide a SET stack to give its customers a significant lead in building SET-compliant applications for merchants and consumers. In addition, RSA also announced that it will work closely with industry partners Netscape, Microsoft, Oracle, and others to incorporate SET into popular Web browsers and Internet E-mail packages.

In addition to Visa and MasterCard, other SET development participants included GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems, VeriSign, as well as RSA Data Security.

Details about SET can be found at RSA's website (http://www.rsa.com).

MedPlus & RSA Partnership Could Save Lives, Critical Diagnosis Time, and Healthcare Costs

A new software application that links physicians at one hospital with patient records at another via the Internet will be previewed next week by MedPlus Inc., a bar coding and electronic records specialist for the health care industry.

A prototype of ChartMaxx-WebLink(TM), a new module for MedPlus' ChartMaxx electronic patient record system, was demonstrated at the Health Care Information Management Systems Society Show, March 4 through 7 in Atlanta.

ChartMaxx-WebLink is the first software application in the health information management industry to make vital patient medical record data accessible via the Internet – anywhere and anytime. Patient confidentiality would be maintained through a special security clearance code.

With ChartMaxx-WebLink, physicians can get more information faster to make important health care decisions. Access to patient records will provide important baseline comparisons to speed diagnosis and avoid unnecessary duplication of medical procedures, especially in away-from-home emergency situations.

The product would help physicians and hospitals save money and deliver better care. and could potentially save lives. Health Data Management last year reported that 80,000 preventable deaths may occur annually from medication errors. Error prevention was listed as one of the chief ways electronic medical records could provide benefits in optimizing care.

"ChartMaxx-WebLink could revolutionize health care delivery," said E. Andrew Mayo, MedPlus executive vice president. "Physicians will have quick access to vital patient information, regardless of location. When timing is critical, this availability of clinical information will improve patient care and help save lives."

Although security modifications are likely by MedPlus and by individual participating hospitals, the system, as designed, protects patient confidentiality by confirming physician authorization. Temporary passwords give "read-only" access to a limited set of documents for specific patients for a limited time (15 to 30 minutes). RSA is working with MedPlus to develop encryption and authentication protocols.

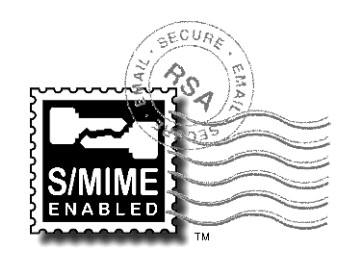
According to a recent issue of Modern Healthcare, "The automated patient record, still in its infancy as a market force, will leapfrog over today's business and billing-oriented software to become the dominant health care information systems category within five years."

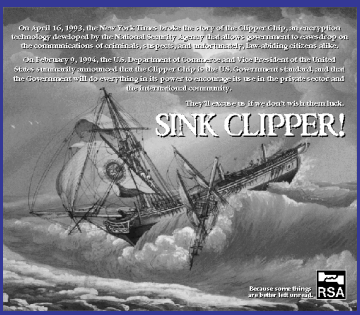
Beta testing is expected to begin in the fourth quarter of 1996. Cincinnati-based MedPlus has over 500 health care clients and is the health care industry leader in bar coding and optical-based archival and retrieval systems.

More information can be obtained from MedPlus by calling 1-800-595-0218.

Visit RSA's Online Art Gallery Today!

RSA's creative team has been hard at work, and now, for the first time ever, you can get your hands on all the terrific RSA posters, logos and artwork. Visit the RSA Art Gallery at *http://www.rsa.com* where you'll find all of the following items for free downloading.





Pacific Rim Ventures

Continued from page 3

toolkits with no restrictions on key size, which is a first," said Bidzos.

RSA also announced that the government of the People's Republic of China will use and distribute RSA products in China. A joint announcement was made today by RSA Data Security, Inc., the Computing Center of the Ministry of Foreign Trade and Economic Cooperation (MOFTEC) of the People's Republic of China, and the Chinese Academy of Sciences Graduate School's Laboratory of Information Security (LOIS), describing an appointment of MOFTEC/LOIS as RSA's exclusive representative for RSA security products in the People's Republic as well as cooperative research and development between RSA and LOIS.

This unprecedented relationship marks a significant step in the globalization of electronic commerce and brings two of the world's leading crypto research organizations together to review and improve cryptographic algorithms and techniques.

MOFTEC is responsible for managing all importers and exporters in China as well as key trading partners worldwide. This is accomplished via a worldwide computer network operated by MOFTEC through which export law, quotas, and taxes are delivered electronically. RSA will deliver its RSA Digital Signature authentication technology, as well as data encryption technology, as allowed by US export law, to MOFTEC for use in securing its network.

In October of last year, James Bidzos, RSA's President and Chief Executive Officer, visited Beijing at the invitation of MOFTEC to provide the keynote address at a MOFTEC-sponsored symposium on electronic commerce. The symposium was widely attended by Chinese government officials, crypto researchers, and members of the business community. The move towards electronic commerce in China and the need to secure the transactions, made obvious at the symposium, brought RSA, LOIS, and MOFTEC into further discussions.

"The flow of commerce in China is rapidly becoming computerized. The integrity and security of our network is of critical importance to the economic efficiency, viability, and national security of the People's Republic," said Dr. Yanping Hu, Deputy Director General of MOFTEC's computing center.

"International standards for security and financial transactions based on RSA, such as ISO 9796 and the recently announced VISA-Master Card specification, are important to us," he added.

"MOFTEC has recognized the need to secure their network and is taking steps now to protect it," said Mr. Bidzos. "By using well-established international standards, MOFTEC and RSA are taking a giant step toward global electronic commerce. While the efforts of the Clinton administration to develop a National Information Infrastructure, or NII, represent a noble ambition, it is clear that global electronic commerce is the future. Commerce is international, and the Internet knows no borders."

The relationship with LOIS has three parts. First, LOIS and MOFTEC will work to "localize" RSA products so that they are suited to the Chinese market. Second, LOIS will develop, in China, a new cryptographic implementation for RSA for use around the world. In addition, LOIS will conduct research in areas of cryptography important to RSA and MOFTEC, including review of current RSA technology as well as new cryptographic techniques.

Professor Zhanseng Zhao of LOIS, an accomplished and respected researcher in artificial intelligence and cryptography, said: "Both academic research and electronic commerce share something in common – they should be independent of national boundaries. We are pleased to participate in these efforts with RSA and MOFTEC."

The Ministry of Foreign Trade and Economic Cooperation (MOFTEC) of the People's Republic of China has a function similar to that of the US Department of Commerce. LOIS (Laboratory of Information Security) is part of the Chinese Academy of Sciences Graduate School.

tion, the latest on VeriSign's S/MIME compliant secure email packages for the Internet, new hardware-based security for SSL from Atalla, and V-ONE's launch of SmartGate, the industry's first security middleware product.

Not to be outdone, RSA also took to the stage with some important annoucements of its own. The debut of the "Genuine RSA Encryption Engine" logo was exciting for both RSA and the many companies who license and incorporate RSA encryption technology into their products (please see article on page 5). The Genuine RSA logo is the first quality assurance symbol offered by the security industry, and will always be the only one backed by the undisputed leader in cryptography.

The latest RSA-sponsored cryptography initiative, called S/WAN, was also officially introduced to the public (please see article on page 4). Both S/WAN and S/MIME, another RSA-sponsored security protocol, have been endorsed by many industry leaders and the first products supporting the S/WAN specification are expected in the first quarter of 1996.

RSA also introduced the latest upgraded versions of its flagship products, BSAFE and RSA Secure. The BSAFE encryption engine in particular has undergone a major upgrade and will play a central role in RSA's strategy to develop the next generation of secure product design architecture (please see article on page 3).

The 1996 Conference featured a Navajo theme in honor of the Native American "codetalkers" employed by the U.S. military during World War II to relay operational orders in the Pacific theatre. The Navajo language seems to have no linguistic connections to any other language, Asian or European, and is so unique that the codetalker program provided a code which the Axis powers were never able to decipher. RSA recognizes that the need for secure communication in a public arena is just as important to today's business "warriors."

"The *sine qua non* of crypto conferences..." – Computerworld

Computer World called the RSA Data Security conference "the *sine qua non* of crypto conferences" — and our plans for 1997 are even bigger! Watch for developments in upcoming issues of Ciphertext – and don't forget to register early!

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 © 1996 RSA Data Security, Inc. All rights reserved. For reprints, call your RSA representative.