Entrust®

KEY Notes

February–March '97

NEWSLETTER

ORCHESTRATING ENTERPRISE SECURITY

The newsletter for organizations and individuals who are serious about computer security

Welcome to Entrust Technologies!

By John Ryan - Chief Executive Officer

I would like to extend a warm welcome to all of our customers and business partners from our new company, Entrust Technologies. As you may know, Nortel spun-out the Secure Networks business unit to form Entrust Technologies on January 2, 1997. As Chief Executive Officer, I would like to explain what this means to our business.

Entrust Technologies will be a majority-owned subsidiary of Nortel, continuing the business of Secure Networks. The Nortel business unit has proven itself to be a leader in enterprise security products and technology since its inception over three years ago. The spin-out was conducted to take advantage of the growing market for enterprise security products. Leading investment firms have recognized the potential of this new company and have invested an aggregate of $26 million. These investment firms include Olympus Partners, J.P. Morgan Investment Management, Société Générale Investment Corporation, T. Rowe Price Threshold Funds, and Donaldson, Lufkin & Jenrette Securities Corporation.

A strong group of people will lead Entrust Technologies. They include Brian O'Higgins, Executive Vice President and Chief Technical Officer; Brad Ross, Executive Vice President, Marketing and Product Line Management, Dr. Paul Van Oorschot, Chief Security Architect, and our team of world-class experts in cryptography and research.

The security market, and in particular the market for public-key cryptography, is growing rapidly as a result of corporate use of the Internet and intranets. According to some recent studies, this market is estimated to grow from $1.1 billion to $16.1 billion by the year 2000.

Our mission is to provide public-key infrastructures and technology to satisfy security requirements for corporate networks, intranets and the Internet, and to continue our strong commitment to superior customer service and support.

It is important that we continue to foster the entrepreneurial spirit so characteristic of this market and that we continue to provide security solutions that meet our customers' requirements.

Your feedback is important to us, so please continue to send us your comments on our products.

We look forward to working with each of you and helping you meet your 1997 business needs.

John Ryan, CEO

Inside:

www.entrust.com
visit the Entrust Technologies *redesigned* Web site

Entrust Technologies

Public-Key Technology Meets Corporate Needs

By Brad Ross - Executive Vice President , Marketing and Product Line Management

Confidentiality of data and strong *authentication* of users are critical requirements in meeting the rapidly changing needs of corporate computer security. Public-key cryptography is widely recognized as the enabling technology for confidentiality and authentication in the distributed computing environment.

Many corporations are discovering that deployment of public-key technology demands an infrastructure to support the public-key certificates and keys that establish the credentials of each user. A certificate includes the public key of the user, signed electronically by a trusted third party, known as a Certification Authority. This signature is used to verify that the public key belongs to the person named in the certificate.

Certificates need to be managed if network privileges are to be controlled. For successful deployment in a corporate environment, certificates and keys should be created, distributed, updated, audited, revoked, backed up, recovered, cross-certified, and integrated with existing systems. In many ways, certificate management is actually more of a networking and directory challenge than a cryptographic one.

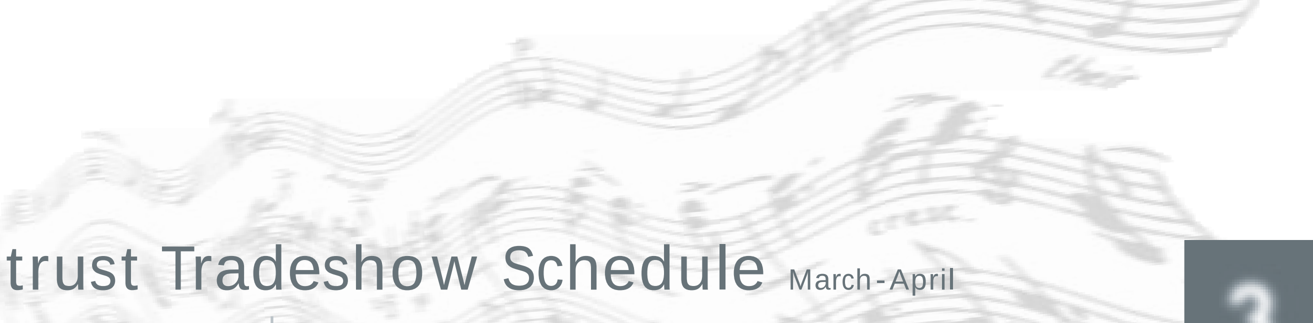
The Entrust family of products is the first commercial key and certificate management system. It establishes a new application category called *public-key infrastructure*. Entrust provides an affordable platform for distributed computing security. It allows corporations to scale public-key management to the level required by their organizations. On the server side, Entrust/Manager™ creates and administers certificates which are then distributed via standards-based directory systems that support the LDAP protocol. On the client side, Entrust/Engine™ performs encryption, digital signature, and key management operations in support of a wide variety of applications.

Entrust Technologies was one of the first public-key algorithm licensees. Entrust Technologies is actively involved in open standards related to public-key technology, such as Version 3 X.509 certificates and the Internet standard APIs and security mechanisms (IDUP-GSS-API, SPKM, GSS-API) that developers use to incorporate security into their applications. With this range of expertise, Entrust Technologies is focused on furthering public-key infrastructure products and technology.

Entrust RAVE REVIEWS

"...the market for PKI products is expected to grow from about $30 million to more than $500 million by 2000. 'Nortel/Entrust stands to play fairly significantly in that market,' said Jennifer Pigg, vice president of data communications at the Yankee Group, a Boston technology research firm." — The Dallas Morning News (January 3, 1997)

"Northern Telecom Limited formed a new company, Entrust Technologies Inc., to make security software that protects the transmission of data over the Internet and corporate networks... Northern Telecom said it values the new company at $90 million to $100 million." — The Wall Street Journal (January 3, 1997)



Entrust Tradeshow Schedule March-April

Show	Date	Location
Open Systems Security	March 17-18	Hilton at Walt Disney World Village, Orlando, FL Booth #21
Internet and Electronic Commerce	March 18-20	Jacob K. Javits Convention Center, New York, NY Booth #1068
EMA (Electronic Messaging Association)	April 7-10	Pennsylvania Convention Center, Philadelphia, PA Booth #717
Please check our Web site for updates to our tradeshow schedule. We look forward to seeing you!		

Entrust Training 1997 Public Course Schedule

Entrust Administrator Training (2 days)

February 11-12
March 18-19
April 15-16
May 17-18
June 17-18
July 15-16
August 12-13
September 16-17
October 14-15
November 18-19
December 16-17

Entrust/Toolkit (1 day)

March 20
May 15
July 17
September 18
November 20

Location:

Unless otherwise notified, all public courses will be delivered in the Entrust Technologies facility in Ottawa.

Course Hours:

All courses run from 8:30 a.m. to 4:00 p.m.

For More Information:

Visit our Web site, www.entrust.com, or send an e-mail to entrust@entrust.com for course overviews, outlines, and pricing, as well as up-to-date scheduling and registration information.

Entrust RAVE REVIEWS

"Entrust's products for developing public-key infrastructures and digital signatures, targeted at business-to-business transactions, enable users to build a single security network capable of growing along with their enterprise networks..." — PC Week Online (January 2, 1997)

"The Entrust software plays a tremendous role in the industry. It's the only product on the market that is as far along, scalable, and [so] robust," said Erica Rugullies, analyst with the Hurwitz Group." — CNET (January 2, 1997)

Entrust Value Added Resellers

By Walter Allan - VAR Sales Manager

Entrust Technologies has a Value Added Reseller (VAR) program that has been operating since the spring of 1995. The program is global in scope, with coverage in the US, Canada, Europe, Asia and Mexico.

Entrust Technologies selects VARs based on stringent criteria, so customers can have confidence in dealing with them. VARs are provided with pre- and post-sales support, including ongoing training, new product release information, and access to key Entrust Technologies management personnel.

VARs enhance the promotional efforts of Entrust Technologies in building brand awareness and goodwill for Entrust. As well, they extend the total product and service solution sets for customers. For example, the first Entrust Users Group was established as the result of a VAR's initiative. VARs can provide comprehensive security solutions, including:

- application integration
- project management
- security consulting
- security audits
- systems integration
- firewalls
- access control
- virus control
- operations

VARs are instrumental in the deployment of Entrust-based solutions, providing a service which adds value to our customers.

Please visit our Web site at www.entrust.com/partners for a current list of Entrust VARs.

Introducing: Entrust Technologies Partner Program

By Lisa Meranger - Partner Program Manager

In early 1997, Entrust Technologies will launch a formal marketing program initially intended to support developers who use Entrust/Toolkit™ to make their applications ‘Entrust-aware’™. The program will support the addition of other types of partners such as resellers, and will offer unique features to support these relationships.

The time is right to start such a program. The recent announcement of the formation of Entrust Technologies as a separate Nortel subsidiary will allow us to take Entrust’s leading position in the enterprise security market to the next level.

Our mandate in the program will be threefold: to make our technology attractive to partners, to equip our partners with the sales and marketing tools they need, and to increase our partners’ visibility in the marketplace.

The feedback from our partners to date has been very positive. Many partners have requested specific marketing activities to pursue with us. It's this level of enthusiasm that will make our program a success.

The program

We have taken a look at other programs in the industry to define additional incentives beyond the standard offerings that partners have come to expect from such programs. Our primary focus will be to provide a unique program that will help our partners successfully market their Entrust-aware product offering. Entrust Technologies will offer equal joint marketing opportunities to all partners.

Co-marketing

Some exciting initiatives are currently under way with our partners, such as promotions on our Web site, participation in marketing events, public relations assistance, a logo program, and more!

Watch for the formal roll-out of this program in the next few months.

Attention Entrust-aware Application Developers!

If you have made an application Entrust-aware for either in-house use or as a third party vendor, we would like to hear from you. We will be highlighting an Entrust-aware application in future issues of our KeyNotes newsletter. This is an exciting opportunity to profile your product to customers, prospects and partners!

To qualify, complete the online form in the Developers' Corner on our Web site: **www.entrust.com/corner.htm**

Developers' Corner

User Applications

The following is a list of additional functions that you should consider when making your application Entrust-aware with Entrust/Toolkit™. Many of these examples are shown in the applications provided with the Entrust/Toolkit documentation.

EntrustFile

- Create new Entrust user profile
- Recover user profile
- Token usage and profile selection
- Select Entrust user profile or token
- Password entry
- Display user information such as user DN and CA
- Display Entrust version number
- Check for mode: full Entrust, Entrust/Lite, or off-line
- Directory search functions for full Entrust and Entrust/Lite
- Directory search functions for personal address book (PAB)
- Recipient display and selection for full Entrust and Entrust/Lite
- Recipient display and selection — personal address book
- Recipient display and selection — private and shared recipient lists
- Display validated and invalidated recipients
- Invalid recipient reason display
- Encryption algorithm selection
- Export user's public certificate
- Import user certificates for users outside your own CA
- Revalidate password after defined time period of keyboard inactivity
- Display and inspect certificate contents during signature verification process
- Display CA name during signature verification process
- Test signatures in a cross-certified environment
- Display error messages when certificates have been revoked
- Display warning if CRL was not available (for example, off-line operations)

If there is an issue you would like to see addressed in this section, send an e-mail to entrust@entrust.com

Entrust RAVE REVIEWS

> "Growing demand for enterprise-level security software has prompted Northern Telecom Limited to spin off its Secure Networks business unit into an independent company. The new company, which is a subsidiary of Nortel and will be called Entrust Technologies Inc., will be a more nimble competitor to other players that provide encryption and digital signature software for corporate networks, intranets and the Internet..." — Communications Week (January 6, 1997)

Building a Public-Key Infrastructure: In-source or Out-source?

Extracts from an article by Dr. Tim Moses - Manager, Security Technology Group

A public-key infrastructure will become increasingly important to every organization's efforts to decrease information processing costs and improve performance. It is well known that automated information systems simplify information processing and eliminate extra data entry. However, unless implemented with care, automation can also increase an organization's risk of loss due to errors and malicious actions by both insiders and outsiders.

While these are serious concerns, mature product solutions do exist to address them. If administered properly, these solutions can provide more assurance than traditional business controls, and they do not affect the cost-savings and performance improvements expected from automation. A public-key infrastructure will be an essential part of any such solution.

Equipment for infrastructure services can be procured and operated by the IT unit within an organization (in-sourcing), or services can be purchased from an external service provider (out-sourcing). This choice involves a number of considerations, and economics may turn out to be one of the more minor ones. Other considerations include the confidentiality and availability of critical corporate information, control over critical system resources, enforcement of agreed obligations, and the quality of service perceived by customers.

Examining the Considerations...

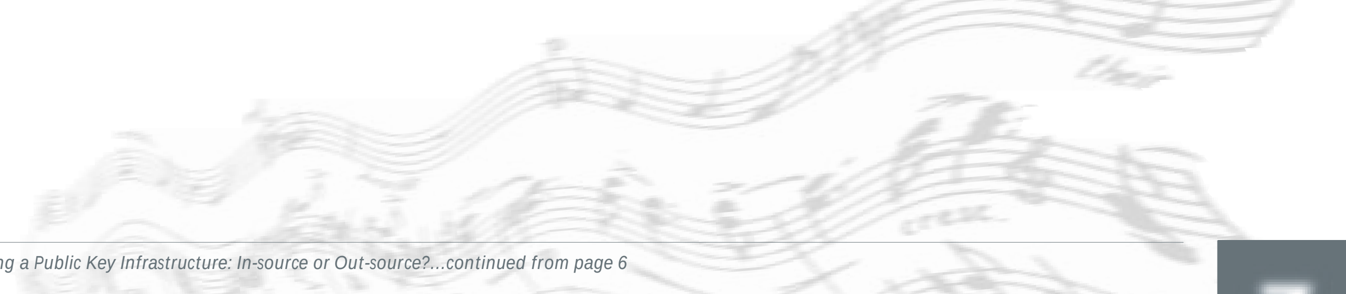
Availability: As more of the corporation's business processes are moved from paper to electronic media, the public-key infrastructure will play a more central role in the organization's operation. Among the most critical operations for a public-key infrastructure are the mechanisms for revoking privileges, issuing certificate revocation lists (CRLs), distributing CRLs, and auditing and archiving the record of the infrastructure's operations. These operations must continue to function smoothly and correctly in order that the organization itself can continue its business processes without interruption. If an out-sourced service provider is used, some guarantee of continued and correct operation must be provided, along with a convincing demonstration that such uninterrupted operation has been available in the past to this or to other organizations.

Liability: In general, the issue of liability does not arise when an organization operates its own public-key infrastructure and trusts only its own certificates. There may, however, be situations in which the organization elects to trust certificates issued by the organization's trading partners. In such cases, the assignment of liability can be controlled by a cross-certification agreement, in very much the same way that conventional trading partner agreements address this issue.

A cross-certification agreement should clearly define how liability is assigned in the event that a certificate's representation turns out to be false or misleading. Generally, a service provider will agree to accept liability only if it can be demonstrated that it deviated from the practices documented in its Certification Practice Statement. If an out-sourced provider is unable to present credible audit records which demonstrate adherence to those practices, then liability is likely to be assigned to it. If it adhered to its practices, but things went wrong nonetheless, it is likely to be held blameless. In the case where the service is in-sourced, however, this vulnerability is comparable to that commonly assumed in traditional business relationships, so it represents no abnormal liability for the corporation.

Enforceability: If a CA is operating properly but a certificate misrepresents the authority of the holder to act on behalf of the organization (due to the holder's fraudulent act), the trust relationship between the issuer and holder of the certificate is important in enforcing the certificate. In such a situation, if the issuing CA is owned and operated by the organization, the organization itself already has a trust responsibility and the certificate may be enforceable against the issuer as well as the certificate holder. If, on the

...continued on page 7



Building a Public Key Infrastructure: In-source or Out-source?...continued from page 6

other hand, an out-sourced service is used, then there is no redress against the issuer. This is because the issuer has committed only to operate within its published practices, and therefore bears no responsibility regarding the certificate holder. The only available course of action is against the certificate holder.

Confidentiality: Generally, registration involves reference to sensitive corporate information; in the case of an out-sourced service, the external service provider must be able to confirm the details of this information. In order to do this, it must have access to sensitive data about the corporation's employees and the employees of its trading partners.

Timeliness: Timeliness of CRL issuance is also an issue. If an employee is fired or is hired by a competitor, their privileges must be revoked immediately. Therefore, certificate revocation must be integrated into human resource procedures. If an out-sourced service is chosen, timely response must be guaranteed, but such guarantees are of little consolation if timely response doesn't happen.

Audit: An audit procedure is required to ensure that the certificate issuer continues to adhere to its published practices. Before considering the use of an external service provider, it should be verified that the provider has identified an independent audit organization that can be trusted and that publishes, uninfluenced, the results of its periodic audits. Because the auditor's client is the subject of the audit, the ability of the auditor to act independently must be carefully considered. It may take several consecutive years of stable operation and several issues of an audit report before the auditor's thoroughness and independence can be completely assessed.

Quality of service: Where the subject of the certificate is a client of your organization, the quality of the service by which the certificate is issued and subsequently managed reflects directly on your organization. Where the public-key infrastructure is operated by the organization itself, the quality of that service is entirely under the organization's own control, and problems with service quality that may endanger the client relationship can be given the immediate attention that they deserve. Where the service is out-sourced, direct control is lost, so it is essential to obtain service quality guarantees and to demand a periodic and independent review of those guarantees.

To Sum Up...

Because of the criticality of the service associated with a public-key infrastructure, the competence of the organization to perform the critical operations correctly should be carefully considered. If the IT unit within an organization has successfully demonstrated its ability to operate mission-critical systems (such as an accounting system or a corporate directory system), the issues encountered in operating a public-key infrastructure, in support of inter- or intra-organizational business processes, should be familiar and represent no unusual risk.

Consequential damage resulting from a failure by the certificate issuing body can far outweigh any direct costs. Therefore, if the certification service is out-sourced, the service provider must be covered by credible insurance for consequential damages, and it must be able to demonstrate that the insurance is continuously in effect. Simply entering into a contract with a provider which places liability on them is not enough, because it does not guarantee their ability to assume liability for consequential damages in the event of failure. Even given credible insurance, however, it must be recognized that causing the service provider to go out of business brings no satisfaction when the corporation's critical systems have been compromised.

Finally, it is worth noting that if a public-key infrastructure is required only to support confidentiality, integrity and authenticity services for the organization's own employees, then the considerations are much more relaxed and there is no reason for an organization not to provide its own service.

The full text of this article can be obtained from the Entrust Web site at www.entrust.com/library.htm

For further information on how to establish a public-key infrastructure for your organization, contact Entrust Technologies at 613-765-5607.

Just Announced! Entrust/ICE

By Glenn Langford - Manager, Desktop Applications Development

Security at the desktop

Entrust/ICE™ (Integrated Cryptographic Engine) is a new product from Entrust Technologies. It encrypts folders to secure selected parts of a disk. This means that sensitive information such as personnel files, strategic plans and financial information can be secured without encrypting the entire hard drive. Whether you are traveling with a laptop or are plugged in at the office, convenient security is a must. And with an Entrust infrastructure, there's no need to worry about losing data because Entrust profiles can be recovered if you forget your password.

Entrust/ICE is designed to automatically encrypt files for Windows 95 and Windows NT 4.0 workstation users. Whether a word processor, spreadsheet, graphics, or any other application is used to create files, Entrust/ICE can automatically secure them. It runs in the background, constantly monitoring file system activity and securing files in selected folders.

Entrust/ICE can automatically encrypt files at shutdown and decrypt them at startup (if required). This is ideal for laptop users who are not always connected to their companies' LANs.

Here's how it works:

- select a folder using the Windows 95 or Windows NT Explorer user interface
- select security options for the folder; for example: delete original after encrypting file.
- Entrust/ICE monitors the file system; whenever files are saved or copied into the folder, they are automatically encrypted.

Users can encrypt files for themselves or for selected recipients and files can be automatically copied to a new folder. This is useful for sharing the encrypted content. A shared folder can be set up on the network to contain only encrypted files placed there by Entrust/ICE.

Entrust/ICE can monitor any number of folders on a local computer. Each folder can be set up with separate security options. For example, there might be a "Confidential" folder on the desktop that encrypts information just for the user and deletes the originals. A "Budget" folder can be secured for people in the accounting department. Entrust/ICE can compress files prior to encryption and copy the secured files to a file server.

Entrust/ICE also adds a number of convenient features that make ad-hoc file encryption and decryption simple. A right-click on any plaintext file encrypts it immediately. To open an encrypted file, simply right-click it and select "Decrypt and open…" The file will be decrypted and automatically opened in the associated application. Entrust/ICE is desktop security the user can set and forget.

For more information on Entrust/ICE, please visit our Web site at www.entrust.com/icehome.htm

For information on Entrust or this newsletter, if you would like to contribute an article to Entrust KeyNotes, or for a listing of our Value Added Resellers in your area, please send an e-mail to entrust@entrust.com or visit www.entrust.com

Entrust KeyNotes is published by:
Entrust Technologies Limited, 2 Constellation Crescent, Nepean, ON, Canada, K2G 5J9, (613)765-5607

This information is subject to change as Entrust Technologies reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

PRINTED IN CANADA IMPRIMÉ AU CANADA