



ORCHESTRATING
ENTERPRISE SECURITY

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

Greetings!

By Brian O'Higgins, Director - Nortel Secure Networks

Welcome to the first edition of the Entrust™ KeyNotes newsletter! As Director of Nortel Secure Networks, I am pleased to have this chance to briefly discuss the importance of network security, the newest Entrust software, and our technology partnerships.

As Entrust customers, value-added resellers, and partners, you see the need for network security on a daily basis. Recent media reports have shown the risks businesses face when their network security is inadequate. While these risks are not new, Nortel has the industry-leading security products to address them.

Background

The first Entrust product was shipped in December 1994. Nortel is currently working on the fifth generation of Entrust—before anyone else has a first version of a comparable product. In recent public announcements, customers such as large financial institutions, the Canadian Federal Government, and

technology partners such as IBM and Hewlett-Packard (HP), have clearly acknowledged the quality of the Entrust product family (see inside story on the Canadian Federal Government Public-Key Infrastructure deployment).

Entrust/WebCA

Since 1994, the security market has evolved greatly and now the Internet has become an attractive medium for conducting business. In response to this, Nortel has developed Entrust/WebCA to provide certificates for Web browsers and servers. Browsers and servers represent the first widely-used communications software to understand certificates. Entrust/WebCA is the latest member of the Entrust product family, and I encourage you to read our feature article about this new and exciting product.

Entrust/Toolkit

The goal of Nortel Secure Networks is to be the leading provider of public-key infrastructure (PKI) products. The value of Entrust to customers increases greatly as additional applications take advantage of the PKI. A common security architecture across applications reduces both costs and risks, and it provides a robust, trustworthy networking environment.

Nortel puts substantial effort into its Entrust/Toolkit family of application programming interfaces. These standards-based interfaces allow applications from numerous vendors

Inside:

**Introducing:
Entrust/WebCA**..... 2

**"Entrust-aware"
Defined**..... 3
A brief description of Entrust-aware applications, their advantages, and how they work

**Entrust
User Groups**..... 4

**Calendar
of Events**..... 5
Entrust tradeshow schedule and Entrust training '97

**Exportable
Cryptography**..... 6
Recent developments regarding the issues surrounding exportable cryptography

**Developers'
Corner**..... 7

**Canadian
Government
Chooses Entrust**..... 8
Canadian Federal Government saves millions of dollars



NORTEL
NORTHERN TELECOM

Awarded to Entrust!

See www.entrust.com for a full copy of the review.



Greetings!...continued from page 1

to connect to Entrust. More than 150 vendors have Entrust/Toolkit and are building "Entrust-aware" applications. It is exciting to see more and more software vendors calling Nortel each week to learn how to make their applications Entrust-aware (see the Entrust-aware article on page 3).

Technology partnerships

Although two years ago seems like ancient history now, our agreement with Microsoft in October 1994 to embed Entrust security in Microsoft Exchange demonstrated Nortel's commitment to successful partnerships. Nortel recently announced technology partnerships with IBM, HP, and Tandem. These announcements show Nortel's ongoing commitment to developing partnerships with well-respected, industry-leading organizations.

Nortel is committed to providing the best security products available on the market. The complex research and development that has gone into building Entrust makes us one of the world's leading developers in cryptography, security architectures and international standards—paving the way for true network security. ✪



Brian O'Higgins,
Director - Nortel
Secure Networks

1 Q 1997

KEYNotes NEWSLETTER

Introducing: Entrust/WebCA

By Tracy Shouldice - Product Manager

On November 11, 1996, Nortel Secure Networks announced Entrust/WebCA, the newest member of the Entrust product family. Entrust/WebCA gives Web service providers the tools to establish and maintain a secure Web environment for their communities of trust, including employees, customers, suppliers and other business partners with whom they do business over the World Wide Web.

Entrust/WebCA overview

Entrust/WebCA lets an organization become its own Web-based Certification Authority (CA), issuing X.509 certificates to Web browsers (such as Netscape Navigator and Microsoft Internet Explorer) and servers (such as Netscape Enterprise Server and Microsoft IIS). Using certificates in conjunction with security protocols such as Secure Sockets Layer (SSL) and Secure HTTP (S-HTTP), browsers and servers can authenticate each other and exchange a symmetric key used to encrypt the session data which flows between them.

These "Web certificates" must be issued to browser and server owners by a trusted, third-party CA. Entrust/WebCA provides any organization with the ability to receive certification requests, screen them for approval, and distribute certificates to those who are to be included in the community of trust. All of these operations can be done over the Web using a standard Web browser.

Applications

Web certificates are needed whenever authentication of server and/or browser is needed, or when information flowing across a Web session is sensitive enough that its confidentiality is a must. Examples of applications requiring Entrust/WebCA are virtually limitless. They include:

- Corporate intranets
- Web-based banking/financial services
- Web-based marketing/customer affinity programs
- Electronic shopping
- Information publishing services

Features and benefits

Entrust/WebCA has many useful features and benefits, including:

Increased control: Entrust/WebCA allows you to control the process of issuing certificates and service response times to users.

Cost-effectiveness: Entrust/WebCA is an affordable solution, allowing certificate issuance across browsers and servers at a very low cost.

Ease of use: HTML-based interfaces make Entrust/WebCA easy to install and use.

Standards compliance: Implements standards such as PKCS, LDAP, X.509, and HTML.

Flexibility: Entrust/WebCA comes with many configurable options and settings.

continued on page 3...

Relationship with Entrust


Entrust/WebCA is built on Entrust technology, using a subset of the features in the current Entrust product. However, it is important to understand that today's commercial browser/server owns its own RSA key pair and performs its own cryptographic operations. Because of this, certain key management functions normally supported by Entrust/Client desktop software—such as automated key rollover and CRL checking—must be performed by the browser/server product instead.

A customer starting with Entrust/WebCA as a Web security solution will be able to upgrade to a full Entrust system capable of issuing Entrust electronic identities and Web certificates, signed by the same Entrust CA. This upgrade is planned for mid-1997. Stay tuned to www.entrust.com for more details.

Pricing and availability

Entrust/WebCA is planned for commercial release in 1Q 1997 at a price of US \$850.

Entrust/WebCA will initially run on the Windows-NT operating system (version 3.51 or better). Support for other platforms, such as Solaris and HP-UX, will follow.

Entrust/WebCA Home Page:
<http://www.entrust.com/webca/webca.htm> 

"Entrust-aware" Defined

A brief description of Entrust-aware applications, their advantages and how they work

by Michel Ranger - Entrust Applications Product Manager

Many vendors provide Entrust-aware products. But what does the term "Entrust-aware" mean? And what are the advantages to customers?

An application becomes Entrust-aware by using one of the various Entrust/Toolkit products to interface to one or more services provided by a pre-installed Entrust/Engine. For each member of the Entrust/Toolkit product family, there is a corresponding member of the Entrust/Engine family (for example, there is an EntrustFile Toolkit and an EntrustFile Engine). Currently, the various Entrust/Engines are:

- EntrustSession Engine
- EntrustFile Engine
- EntrustIDUP Engine for S/MIME

The number of interfaces Entrust provides will grow. For the most up-to-date list, please check the Entrust Web site.

Entrust-aware advantages

Entrust/Toolkit lets application developers rapidly build and deploy scalable security solutions for intranet and Internet applications.

Entrust-aware applications take advantage of the key management services in Entrust (for example, secure key storage, automatic key

update, key backup and recovery, and cross-certification). Because Entrust/Toolkit provides high-level interfaces, it is easy for application developers to add security to their products. For customers, Entrust-aware applications minimize administrative overhead because they all use the Entrust infrastructure. This means that security personnel only need to go to one place to administer a user's security credentials across an unlimited number of applications. And users are able to have a single password across all of their Entrust-aware applications.

How do Entrust-aware applications work?

Entrust-aware applications access security services at run-time through Entrust/Engine. Entrust/Engine represents the run-time implementations of the software interfaces provided in Entrust/Toolkit. Entrust/Toolkit is the software developer's kit consisting of Entrust/Engine, programming documentation, sample applications, sample Entrust user profiles, and the set of header files required to build applications on top of Entrust/Engine.

Through Entrust/Engine, Entrust-aware applications generally communicate with the Directory often to get the encryption public key certificates and certificate

continued on page 4...

revocation lists (CRLs).

Communication with Entrust/Manager is needed for new user creation and key updates, which are relatively rare events.

Entrust client-side software architecture

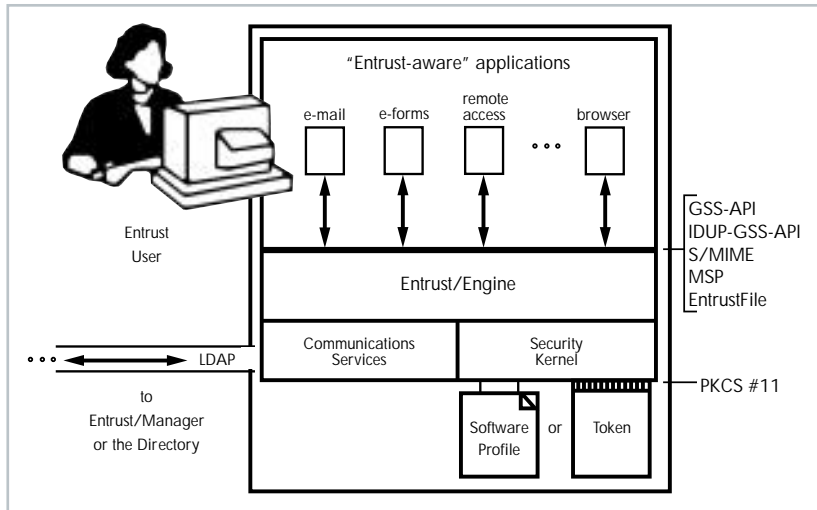
Questions for Entrust-aware application vendors

Security is always a complementary feature for applications. As such, not every application needs all of the security services available from Entrust. For example, some applications may only need digital signature, whereas other applications may need both encryption and digital signature.

Vendors will use these security features to differentiate themselves from other competing Entrust-aware applications. Customers should ask vendors what Entrust features are exercised by their Entrust-aware applications.

Some things to consider:

- How long has the vendor been Entrust-aware?
- What type of after-sales support does the Entrust-aware vendor provide?




Entrust Client-side software architecture

- What Entrust features are used in their applications? Confidentiality? Digital signatures on long-term data? Authentication?

How does an application become Entrust-aware?

Vendors looking to make their applications Entrust-aware need to license and buy one of the Entrust/Toolkit products. The developer then uses the compile-time API to build an application that makes calls to the appropriate Entrust/Engine run-time.

Developers are also encouraged to attend developer training courses and Entrust-aware developers meetings. When possible, Nortel encourages developers to visit our site and describe what their applications are trying to accomplish, as there are cases where a developer may require a consulting engagement for more in-depth assistance.

Nortel often helps and works with the developer's first Entrust customers to ensure customer satisfaction and timely feedback to both the developer and the Entrust team. As the relationship develops, Nortel offers reciprocal sales and marketing programs, early beta programs, seminars, and introductions to Entrust User Groups, customers, and other Entrust partners. 

Entrust User Groups

There are currently two Entrust User Groups, one in Ottawa and another in New York City. The purpose of these groups is for our customers to meet regularly to discuss security issues within their organizations, including ways in which they use Entrust. User Groups are established based on demand in a particular location.

Get involved—if you would like to establish a user group in your area or would like more information, please send an e-mail to entrust@entrust.com 

Entrust 1997 Tradeshow Schedule

Show	Date	Location
<i>RSA Data Security Conference</i>	January 28-31	Masonic Auditorium, San Francisco, CA Booth #5
<i>Open Systems Security</i>	March 17-18	Hilton at Walt Disney World Village, Orlando, FL Booth #21
<i>EMA (Electronic Messaging Association)</i>	April 7-10	Pennsylvania Convention Center, Philadelphia, PA Booth #717
<i>NetSec</i>	June 9-11	Hyatt Regency Hotel, San Francisco, CA Booth #304
<i>ITxpo</i>	October 7-9	Walt Disney World Dolphin, Lake Buena Vista, FL Booth #443
<i>CSI (Computer Security Institute)</i>	November 16-18	Sheraton Washington, Washington, DC Booth #406

Please check our Web site for updates to our tradeshow schedule. We look forward to seeing you!

Entrust Training January-June 1997

Entrust Administrator Training January 14-15 February 11-12 March 18-19 April 15-16 May 17-18 June 17-18	Entrust/Toolkit Training January 16 March 20 May 15	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.
	Course Hours: All courses run from 8:30 a.m. to 4:00 p.m.	

Make Entrust training part of your 1997 security strategy.



“This is some of the most usable security software we’ve seen. The Entrust/Client software is extremely fast, typically taking less than two seconds per file.” — Network Computing (November 1, 1996)

“Entrust/Lite is a solid, user-friendly product. So if security is on your mind, keep Entrust on your short list.” — Computer Shopper (July, 1996)

Exportable Cryptography

Recent Developments Regarding the Issues Surrounding Exportable Cryptography

by Dr. Paul C. Van Oorschot - Chief Security Architect

The status quo

The present laws regarding the legal export of products that include cryptographic functionality is essentially the same in Canada and the United States. These laws require export licenses to be acquired. Such licenses need varying degrees of paperwork depending on the situation. Export licenses are generally granted, with few exceptions, for products that limit lengths of keys for symmetric encryption (for example, DES, CAST, RC2) to 40-bits, and to 512-bits for public-key algorithms for encryption or key management (for example, RSA key transfer or Diffie-Hellman key agreement).

Export controls are less of an issue when the end-purpose of the cryptographic service is authentication only; exported message authentication code (MAC) algorithms may use more than 40-bit keys, and public-key signatures (for example, RSA and DSA) using 1024-bit keys are widely used. Export restrictions are relaxed for international branches of North American-headquartered corporations. In this case, export of a North American product is typically allowed for use within the corporation. In cases where the

cryptographic strength of the exportable product is limited, innovative architectures and key management protocols—such as those used within Entrust—allow interoperation between the domestic and exportable versions without affecting the security of the domestic product.

Times of change

The first widely-circulated public notice of the coming “new world order” for exportable cryptography was the statement from the office of U.S. Vice-President Al Gore on October 1, 1996. Since Canadian export policy is generally in line with U.S. policy, these developments are important in both countries. The statement itself was more of a policy direction statement than a detailed technical plan, but it nonetheless gave clear indication that there would soon be changes on the export front. While the details remain to be confirmed, the following is a reasonable interpretation of what may unfold.

Starting approximately January 1997 and for a period of two years, U.S. firms may be granted export licenses on a 6-month basis for products offering 56-bit DES encryption functionality. However they are subject to the following condition: vendors must commit to implementing a commercial key recovery functionality within their products (see below). After the two-year period, this key-recovery functionality will be mandatory for export of products that incorporate 56-bit DES. Moreover, after this period, controls may be relaxed to allow export of unlimited key-length symmetric encryption, given the presence of a key-recovery functionality.

Key escrow, key recovery, and plaintext recovery

The details of the required key-recovery functionality have yet to be finalized. Commercial key recovery differs from key escrow in the following way. In key escrow, as originally proposed in the U.S. Government Clipper proposals (which suffered unprecedented public rejection), copies of each end-user’s long-term secret keys were effectively kept “in escrow” by a number of third parties. The third party would surrender these keys to law enforcement officials upon a court order that authorized wire-tapping.

continued on page 7...



“Entrust is one of the most thorough encryption and key-maintenance systems available.”

— Byte Magazine (May, 1996)

“Operating nearly transparently, Entrust is among the few products to come close to achieving the goals of security and convenience.” — LAN Times (November 11, 1996)

In contrast, commercial key recovery, whereby a user's own organization keeps a backup copy of each user's long-term encryption keys, is now widely recognized as a commercial requirement. It allows key recovery when users lose their own local copies or leave the organization under unfavorable circumstances. Without key recovery, an organization might lose access to critical corporate information encrypted on the user's local platform. In fact, key recovery itself is not the actual commercial requirement, but rather plaintext recovery: given the ciphertext, an organization must be able to recover the corresponding plaintext. Thus a user's private decryption key need not be exposed to meet the functionality needed by legal wire-tapping orders. It is now being recognized that plaintext recovery is the solution which meets both government and commercial requirements.

Key recovery in Entrust

Since its inception, the Entrust product line has provided a backup and recovery strategy by which an end-user's decryption private keys are backed up in Entrust/Manager.



"The speed and strength of Entrust's encryption, together with the automatic handling of key management and document verification, make it both easy and powerful enough to get a high level of security practical for any organization." — Network World (March 11, 1996)

(There is no reason to back up signature private keys; if lost, new keys can be regenerated without consequence. Moreover, backing up signature private keys causes the loss of legal grounds on which to base a non-repudiation service. A two-key pair system with separate encryption and signature key pairs is now recognized as a commercial requirement.) Thus, Entrust already provides much of the functionality recognized by the "new world order". Nortel will track new export developments as they unfold, and Entrust will evolve to meet new export laws on products of maximum cryptographic strength.

Industry alliance

Nortel has joined an industry alliance spearheaded by IBM, including other key players such as Hewlett-Packard, and Trusted Information Systems. This alliance is working towards a common set of commercial solutions that will provide key or plaintext recovery functionality. The alliance is also working towards meeting the needs of both domestic and international consumers using maximal-strength cryptography, and will be in line with government requirements. ✪

Developers' Corner

Welcome to Developers' Corner—here we regularly provide Toolkit developers with tips and hints on how to better use Entrust.

Off-line mode

Some applications are designed to work in a remote environment where access to a public directory is not available. This can be the case for both Entrust and Entrust/Lite environments. Application performance can be enhanced by using "off-line" mode. In this mode, Entrust-aware applications do not try to connect to the public directory. The Entrust/Engines will acknowledge that the application is in "off-line" mode with an appropriate return code from the function call.

To set "off-line" mode, make the following change in the "entrust.ini" file:

Entrust/Lite

PublicAddressBook=<none>

Entrust

Server=<none>



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

Canadian Government Chooses Entrust

Entrust saves Canadian Federal Government millions of dollars

By Ian Curry - Entrust Product Manager

Like most government departments, Public Works and Government Services Canada (PWGSC) is concerned about network security. The need for secure electronic commerce and information exchange is becoming paramount to the Department's daily operations.

The Government has incorporated Entrust in its public-key infrastructure (PKI). The PKI allows users to secure local files and network communications for electronic mail, electronic forms, electronic data interchange (EDI), database access, the Web, and many other applications. Entrust provides the enabling technology required to meet future security goals and objectives within the government.

Government Telecommunications and Informatics Services (GTIS), a branch of PWGSC, has implemented an Entrust-based PKI to provide

improved security for a variety of common applications. GTIS will implement all the features and functionalities required in a robust key management service.

Efficiency from technology


By implementing a PKI which can be used by other government departments, GTIS can help the federal government obtain the benefits of improved network security. This will also help to reduce the reliance on paper-based transactions, saving millions of dollars and improving efficiency.

Why Entrust?

The PKI will support the latest products built to emerging commercial security standards. A broad range of vendors will be able to incorporate Entrust security into their applications to make them compatible with the government PKI.

Reliability and availability

The GTIS PKI operates 24 hours a day, 7 days a week, to support departmental use of the service. Reliability and availability are ensured through best-in-class redundant hardware and software configuration, duplication of X.500 directory data, and daily system back ups.

GTIS is building on accepted international standards to bring high quality, easy-to-use security to government information and transaction processing. The GTIS PKI provides the fundamental security required to be a major player on the information superhighway, and Entrust ensures the Government of Canada will be a leader in secure information technology. 



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:
Nortel Secure Networks, 2 Constellation Crescent, Nepean, ON, Canada, K2G 5J9, (613)765-5607

All contents Copyright 1996, Nortel. All rights reserved. Entrust is a trademark of Northern Telecom Limited. All other product and company names are trademarks of their respective owners.

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

