



Exocom Builds Security Solution for Large Service Company

ORGANIZATION

Large Service Company

CHALLENGE

To develop a cost-effective, scalable, user-friendly database application for consolidating confidential data from franchise offices to build a single corporate database.

SOLUTION

Exocom Technology Solutions –
Professional Services
Entrust Technologies –
Entrust/PKI™
Entrust/ICE™
Entrust/Toolkit™

RESULTS

EXOCOM and the company's Security Manager installed and configured Entrust/PKI, an X.500 directory, the authentication server and assisted with integration of the remote access product.

The result is an integrated solution with a single interface that has automated and secured inter-company communications.

EXOCOM Technology Solutions has completed the implementation of an Entrust® public-key infrastructure (PKI) for the head office of a large service company. This framework provides the head office and its franchises with a security architecture for exchanging sensitive information over the Internet. The company is also using this security infrastructure, in conjunction with Entrust/ICE™, for protecting information on the company's desktop computers. For reasons of confidentiality and security, the company has requested anonymity.

Customer's Objective

The company embarked on the development of a distributed database application for capturing confidential information at the franchise offices. Using standard database replication, the company planned to capture and consolidate information from its franchises into a single corporate database. The communications infrastructure for this database needed to support the daily exchange of high volumes of information and to be assembled in a manner that encouraged the franchises to participate. To satisfy these requirements and to keep communications costs under control, the company needed efficient communications and a system that minimized user intervention.

Solution

The Internet was selected as the most cost-effective solution for communicating with its franchises. Deals were made between the company and several Internet Service Providers, which will fix the costs at a minimum. A routed Internet connection and a firewall were installed at the head office to protect the network. The franchises use dial-up connections.

The company selected a remote access product to provide scripted exchange of information. However, the implementation of automated database replication over the Internet raised concerns with the company's Security Manager, specifically with the authenticity and confidentiality of the data traveling over a public network. He was also interested in implementing a corporate security strategy that would integrate with the other informatics and



security initiatives being planned. The security solution to be adopted had to be flexible in the event that the company acquired or lost franchises, or implemented other applications needing security.

The company contacted EXOCOM because of its experience with secure remote access solutions and status as an Entrust Partner™. After gaining a more detailed understanding of the company's requirements and its need for flexibility in the security solution, EXOCOM suggested using Entrust for user authentication and to encrypt the Internet TCP/IP traffic. EXOCOM had been working extensively with a number of technologies as part of its secure remote computing solution.

EXOCOM was awarded a contract with the company to implement a pilot of an Entrust public-key infrastructure, including the installation and configuration of Entrust, the X.500 directory, the authentication server and assistance with the integration of the remote access product. EXOCOM sent a small team of engineers to install the solution and to help smooth out some of the integration issues with the company's environment. During the implementation, EXOCOM worked closely with the Security Manager and provided the company with training on each of the products involved, knowledge transfer on their specific implementation, and access to the product development teams.

Advantages and Benefits

The company's pilot lasted about four months, during which it tested the reliability and integrity of the solution. EXOCOM coordinated the development on minor enhancements to some of the products, to provide for a more tightly integrated solution that automated inter-company communications. EXOCOM also provided assistance to the company's development team in their efforts to construct a single interface.

The Entrust PKI pilot proved successful and the company has now contracted with EXOCOM for all the products and for annual support and maintenance. The upgrade of the pilot to full implementation was completed remotely, and followed up with a site visit to provide additional training and optimization of the X.500 directory, and a cross-certification test with another Entrust site. The company also acquired Entrust/Toolkit™ and copies of Entrust/ICE for its desktops. It is already looking at expanding the implementation to include additional franchises and a fully redundant infrastructure.



Federal Government Department Uses Entrust-Ready™ Forms Application to File Documents Online

As the Internet increases in popularity as a medium for doing business, the Investment Review

ORGANIZATION

Investment Review Division
of Industry Canada
<http://www.investcan.ic.gc.ca>

INDUSTRY Government

CHALLENGE

To develop a cost-effective and secure electronic system for investors to submit confidential information to the IRD to replace older paper-based processes.

SOLUTION

General Network Services, Inc.
(GNS) — FormLock
Entrust Technologies —
Entrust/PKI

RESULTS

IRD has moved to an electronic filing system through their Web site. The strict confidential nature of the information is maintained by encrypting and signing (using Entrust®) the body of the form on a local computer and sending it to IRD using a Netscape® browser and the Entrust-Ready™ FormLock™ plugin from GNS.

Division of Industry Canada (IRD) is taking advantage of new technologies to enhance their collection and filing process. The IRD is responsible for administering the Investment Canada Act. This Act requires that foreign investors provide specified information to the IRD when they establish a new business in Canada and when they acquire control of a Canadian business. Up to this point, this information has been provided on paper and submitted to the IRD either by fax, mail, or courier. Depending on the industry and size of the investment, the information may be fairly basic, or in the case of a reviewable investment, it may be quite detailed. All information submitted remains strictly confidential.

General Network Services, Inc. (GNS), an Entrust® Partner, is assisting the IRD in adopting the latest technology to assist foreign investors to provide the necessary information in the most efficient manner possible. Not only will IRD's operating costs be lowered but their clients' turnaround time will be reduced. IRD took the first step to electronic filing of information when it developed its Web site. Standard filing forms are available on this site but it was only through a partnership with General Network Services that IRD is now moving rapidly towards full electronic filing capability. The strict confidential nature of the information will be maintained by having the body of the message digitally encrypted on a local computer (by Entrust software) and sent to IRD using a Netscape® browser and the FormLock™ plugin, a GNS product built to work with Entrust software.



During the pilot phase of the IRD project, a small trial group of the largest users have been fully equipped with Entrust and FormLock. Within the year, all businesses that are required by the Investment Canada Act to provide information and who have access to the Internet will be able to file electronically using the security of Entrust and the FormLock plugin.

Entrust software provides two things: encryption of the secure information, and authentication of the senders. By using Entrust software, IRD is assured that the information it receives is secure and that the sender has been authenticated. With FormLock, Entrust users, like IRD, are able to submit standard Web forms with confidence using the Netscape browser. The sender is guaranteed that their information has not been viewed by people who are not supposed to see it, and the recipient is secure in the knowledge that the information actually comes from the person the submitter claims to be.

To participate in the pilot, all IRD personnel installed Entrust and were provided with keys. Their users in the private sector were also supplied with the same. The FormLock installation program seamlessly installs into an existing copy of Netscape, and from there users have a secure interface for submitting the forms, with digital signature included, ensuring that the submitted information is not altered and providing proof that the information is from the sender.

The primary characteristic of FormLock is that it uses a standard Web form interface. This feature, combined with the security that comes with the Entrust public-key infrastructure, has generated interest in FormLock worldwide.

“We have a test group of law firms and have successfully completed initial trial submissions. We are now in the process of widening the pilot and identifying new participants”

*Tyson Macaula,
Chief Information Officer
General Network Services*



Critical VPN Security Solution: A Cornerstone for the Kansas Bureau of Investigation

ORGANIZATION

Kansas Bureau of Investigation
<http://lawlib.wuacc.edu/ag/kbi.html>

INDUSTRY

State Government
 Law Enforcement

CHALLENGE

Provide solid security for its local network from multiple points, including remote access along with dynamic security and intrusion detection

SOLUTION

Entrust Technologies —
 Entrust/PKI

Check Point Software
 Technologies — VPN-1

Internet Security Systems —
 RealSecure

FishNet Consulting —
 deployment and maintenance

RESULTS

Users of the system will:

- Receive near real-time criminal information regardless of location;
- Provide criminal histories to regional offices economically;
- Provide back-up for the existing frame-relay system, ensuring access to information in the event of technical failure;
- Retrieve criminal histories via the Internet in minutes compared to days or weeks using older technology and processes; and
- Assure that all communications, including e-mail, are encrypted and protected from tampering or wrongful use.

To remote law enforcement officers, the timely profile of a potentially dangerous

suspect could mean the difference between life and death. The Kansas Bureau of Investigation (KBI) is an organization that is committed to improving officers' access to vital information while in the line of duty. Using Entrust/PKI™ solutions and services from a group of security partners, the KBI reaped the benefits of an Internet-based VPN security solution to drastically increase the speed, security and affordability of transmitting criminal histories to remote officers.

Challenges

To create the KBI solution, several technical challenges had to be addressed.

The VPN system needed to provide solid security for its local network from multiple points, including remote access along with dynamic security and intrusion detection. It also had to be extremely fault tolerant while ensuring privacy, security, strong authentication and data integrity in order to meet current FBI requirements regarding Internet security. Finally, it was essential that this solution be manageable and economical enough for many of the small, rural towns in the state.

The Solution

The KBI's requirements for a unique and robust security solution were met by the combined product and service offerings of an important group of security industry partners including:

FishNet Consulting — a leading reseller and integrator of Internet solutions in Kansas — deployed and will maintain the VPN solution.



Entrust Technologies' Entrust/PKI™ and Check Point Software Technologies' VPN-1™ together provide secure, encrypted remote access and authentication for the KBI's VPN solution; and Internet Security Systems' RealSecure™ product provides security intrusion detection for the system.

Results

The KBI's new secure VPN system quickly delivers information to 105 Kansas counties using the state's shared telecommunications network and common ISPs. Currently, the secure VPN application is being used for a 2,500-seat project in the State of Kansas.

The system will be rolled out to accommodate upwards of 12,000 users from 750 criminal justice agencies by the year 2000 and will save the Kansas criminal justice agencies an estimated \$2.5 million per year.

The KBI application is a success story on many levels. It will lead to improved working processes, cost savings and ultimately will improve the safety of law enforcement officers in Kansas and other regions with similar requirements. Further, the applications story serves as an excellent model of the key role of industry partnerships in creating flexible and specific security solutions in a timely fashion.

“The interoperability between Entrust and Check Point products, along with its low cost implementation, were key criteria in our decision to utilize Entrust and Check Point together. On top of that, both products have earned a reputation as premier security providers in the marketplace.”

Ron Rohrer

Information Resource Manager

Kansas Bureau of Investigation

Entrust Saves Canadian Federal Government Millions of Dollars

ORGANIZATION

Government of Canada
http://www.cio-dpi.gc.ca/pki/pki_index_e.html

INDUSTRY

Federal Government

CHALLENGE

Secure local files and network communications for electronic mail, electronic forms, electronic data interchange (EDI), database access, the Web, and many other applications

SOLUTION

Entrust Technologies —
 Entrust/PKI™

RESULTS

- Real dollar savings
- Easy-to-use, standards-based security
- 7 days a week, 24 hours a day reliable service

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 operation.

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 Telecommunication 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 have incorporated Entrust security into their applications to make them compatible with the government PKI.



Reliability and Availability

The GTIS PKI needs to operate 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 more information on the Government of Canada (GOC) PKI implementation activities, point your browser to:
http://www.cio-dpi.gc.ca/pki/pki_index_e.html

"We will make the information and knowledge infrastructure accessible to all Canadians by the year 2000, thereby making Canada the most connected nation in the world

A connected nation is more than wires, cables and computers. It is a nation in which citizens have access to the skills and knowledge they need to benefit from Canada's rapidly changing knowledge and information infrastructure. It is also a nation whose people are connected to each other."

Speech from the Throne

September 23, 1997

Royal Mail Launches ViaCode - the UK's First Secure E-commerce Service for Businesses

ORGANIZATION

Royal Mail —
the postal service for the UK
<http://www.royalmail.co.uk/>
<http://www.viacode.com/>

INDUSTRY

Postal Authority

CHALLENGE

To provide businesses with a new way to conduct business over the Internet safely and cost-effectively with security for Internet e-mail and other commercial transactions.

SOLUTION

Entrust Technologies —
Entrust/PKI™

RESULTS

- Protection of Web sites, to ensure they are tamper-proof
- Electronic identities you can trust

Royal Mail has brought a huge new level of trust and confidence to the Internet with the launch of ViaCode, the UK's first secure e-commerce service for businesses providing, for the first time, rigorous proof of identity.

With ViaCode, Royal Mail's proven reputation for trust is now available to businesses using the Internet. Royal Mail is underlining its record for integrity and security with a guarantee of the reliability of the ViaCode service up to a value of £100,000.

Launching ViaCode at a news conference in London, Royal Mail Managing Director, Richard Dykes said: "Internet use is expanding rapidly. Now businesses can have the best of both worlds by combining Royal Mail's 350-year-old reputation for trust in delivering mail with the Internet's global capability for handling messages, complex documents and commercial transactions."

Unique Security Assurances

In contrast to existing encryption services, businesses using ViaCode will have to provide Royal Mail with strong physical proof of the identity of users. Royal Mail's "certification" process is unique in the UK and provides a high level of assurance and authentication to UK firms and businesses not previously available. Mr Dykes said, "Anyone serious about electronic commerce will have to adopt security practices and techniques of this kind to safeguard their business."



World-Class Service

Jim Pang, Royal Mail Director of Electronic Services, said, “Moving information electronically has long been an option, but not with the same trust and integrity that paper systems can provide. Royal Mail has used the best encryption security technology available to create a world-class service. With ViaCode, computer users anywhere can be absolutely confident about who they are communicating with. They can be certain that the information they send cannot be read by anyone other than the intended recipient.”

Based on Entrust's software, one of the world's most mature and most respected PKIs, ViaCode offers a high level of trust, security and ease of use. The new service will be provided in tailored solutions for individual customers so the price will vary. But for a typical business, ViaCode could cost less than £1 a week for each employee at the company “certificated” to use the service. Mr Dykes said: “ViaCode will be highly competitive and very affordable.”

Additional new features for ViaCode are already being developed. These include providing proof of delivery and proof of submission with Royal Mail vouching that messages have been delivered and opened by the recipient. This service will offer a truly trusted and secure Internet-based alternative to the international, overnight document courier market.

“Royal Mail has used the best encryption security technology available to create a world-class service.”

Jim Pang

Director of Electronic Services

Royal Mail

Entrust and Scotiabank: Securing the Future of Internet-based Electronic Commerce

ORGANIZATION

Scotiabank
<http://www.scotiabank.com/online.html>

INDUSTRY

Banking

CHALLENGE

An easy-to-use Internet-based solution for ensuring secure transactions for the Bank's Scotia OnLine banking and brokerage service using state-of-the-art security with open standards

SOLUTION

Entrust Technologies —
Entrust/Direct™
Hewlett-Packard —
Virtual Vault server

RESULTS

- Web site spoofing eliminated
- Full end-to-end security
- Reliance on browser "add-on" security eliminated
- Single sign-on
- Session control assured
- Bank card number and password are not transmitted over the Internet

The advent of Internet-based technologies has sparked corporate visions of ubiquitous electronic commerce that allows customers to access products and services from their homes, 24 hours a day. But how can companies offer customers the convenience of conducting business over the Internet, while ensuring the most stringent security standards to protect confidential information? This is an especially pressing issue for financial institutions.

For Scotiabank, one of North America's largest financial institutions, an easy-to-use solution for ensuring secure transactions was a prerequisite for its innovative Scotia OnLine service, launched in September 1997. Through a single log-on session, Scotia OnLine lets customers use their Web browsers any time of the day to get up-to-the-minute bank account balances, pay bills, transfer funds — even view their latest VISA transactions and statements, a unique feature. They can move freely between banking and brokerage transactions during the same session, without having to enter separate passwords.

"Customers were asking for the convenience of easy, one-point access to transactions and their account information using their Web browsers," says Paul K. Wing, Vice-President, Systems Security and Controls at Scotiabank. "At the same time, they had to be confident that our system could ensure the privacy and integrity of any personal information and account transactions transmitted over the Internet. As well, we needed to protect Intranet communications by employees of Scotiabank and our subsidiaries operating in more than 50 countries worldwide."



The bank determined that the best-of-breed technology for developing the security solution it required was public-key cryptography. Based on international standards, this technology uses electronic certificates to authenticate customers, and mathematical keys to encrypt and digitally sign each transaction. This technology ensures the integrity and confidentiality of information transmitted over the Internet.

To guarantee the highest possible level of security, Scotiabank required an integrated public-key solution combining encryption and digital signature capabilities with fully automated key management. As well, the solution had to be based on best practices and open standards, and be fully scalable.

To create the secure Internet commerce solution, Scotiabank needed to partner with a vendor of public-key encryption technology. "We asked the question: Who is the technology leader in public-key cryptography?" says Paul K. Wing. "After a year of market research and due diligence, we had a clear answer: Entrust Technologies."

A Record of Success

Entrust Technologies is the leading provider of Certification Authority (CA) and public-key management products. Entrust's public-key infrastructure (PKI) delivers strong encryption, certificate-based authentication and key management services.

Entrust's core competencies and the company's proven record of achievement were a perfect match for Scotiabank, with its 165-year record of sound banking practices. Entrust solutions had already been adopted by a critical mass of government agencies and Fortune 500 companies – Entrust Partner companies like IBM, Netscape, Tandem, Hewlett-Packard, Control Data, Bell Global Solutions and Digital Equipment Corporation. In addition, the Canadian federal government had announced it was using Entrust products to build its own public-key infrastructure that will serve as a Canadian standard.

Entrust/Direct™ – The Unique End-to-End Online Banking Solution

By partnering with Scotiabank to develop Scotia OnLine, Entrust was able to apply this technology to a unique end-to-end online banking security solution, Entrust/Direct™. With Entrust/Direct, banks and other financial institutions can give customers convenient, personalized services via a secure, easy-to-use solution that is more cost effective than other security technologies.

Taking advantage of Entrust's public-key infrastructure and working with the most popular Web browsers, Entrust/Direct offers the same powerful security features developed for Scotia OnLine banking and discount brokerage services — strong encryption, and certificate-based authentication and public-key management.

“Clearly Entrust had what we were looking for,” says Mr. Wing. “So we approached them with a strategic alliance in mind, and posed the challenge: Can you work with us to create, design, and implement this technology for a 1997 launch?”

End-to-end Security – The Key to Customer Acceptance

Entrust more than met Scotiabank’s challenge. In March 1997, Entrust delivered a proof-of-concept prototype for Scotiabank’s review; three months later, it had installed a working solution.

The premise of the system is simple: extend the security offered by Entrust’s public-key infrastructure by installing Entrust software clients on customer PCs and on the Scotiabank Web server, so that these clients together establish a secure session using Entrust’s certificate-based authentication and key management service. Once the session has been negotiated, the Entrust clients intercept all incoming and outgoing messages and automatically encrypt/decrypt them.

Scotiabank issues public-key certificates to customers; with these, customers can encrypt and decrypt data and generate digital signatures recognizable only by the Scotia OnLine Web server. By allowing mutual authentication of the customer and Scotiabank, the certificates eliminate the risk of a spoofed Internet site that looks like the Scotia OnLine service but is aimed at obtaining confidential information about customers and their business with the bank.

To minimize the risk of identity theft, customers choose their own password, which is verified on their personal computer by the Entrust software – it is never transmitted over the Internet. “Unlike most Secure Sockets Layer (SSL) implementations that send users unique access identifiers and passwords over the Internet, our system uses digital certificates to mutually authenticate users and the bank,” says Mr. Wing. “In this way, clients get end-to-end security without needing to understand anything about the technical complexities of the underlying public-key infrastructure. Indeed, the system is very easy to use.”

To access Scotia OnLine from their PCs, customers simply click on the Scotia OnLine icon and enter their password. Within a single session, they can review their accounts, transfer funds, pay bills, set up bill payment arrangements, update their financial portfolio, as well as buy and sell stocks.

A Secure Future for Scotia OnLine

Are customers taking advantage of the convenience of Scotia OnLine services? The answer is an unqualified “Yes”. Scotiabank is the largest digital Certification Authority in Canada and is positioned in the forefront of e-commerce.

According to Mr. Wing, Entrust’s contribution to the initial Scotia OnLine service offerings exceeded Scotiabank’s expectations. “We intend to use Entrust public-key technology to address many more ideas and challenges to allow us to meet our customers changing needs,” says Mr. Wing. “For example, we see a strong demand for complex electronic transactions such as paperless credit applications based on a digital signature, and for electronic transactions that allow both the sender and the receiver to confirm the transaction so that neither party can repudiate it.”

“We asked the question: Who is the technology leader in public-key cryptography? After a year of market research and due diligence, we had a clear answer: Entrust Technologies.”

Paul K. Wing

Vice-President, Systems Security and Controls

Scotiabank

Offering Secure Financial Services over the Internet

ORGANIZATION

US Bank with global reach

INDUSTRY

Financial

CHALLENGE

To build an innovative browser-based platform that provides customers with access to their account information and the ability to conduct financial transactions from a single application.

SOLUTION

KyberPASS Corporation —
VPN technology
Entrust Technologies —
Entrust/PKI™

RESULTS

- Simple and transparent secure application for the bank
- Strong authentication of users
- Provision of encrypted sessions to ensure privacy and data integrity, and audit logging to guarantee non-repudiation of sensitive financial transactions

This profile features one of the largest banking companies in the United States.

This financial institution is widely recognized as a leading technology company and has more primary relationships with large U.S. companies than any of its competitors, making it the leading bank to corporate America. The bank is the provider of choice for more than 10,000 companies and institutions with a presence in more than 52 countries.

Customer's Objective

The bank's main objective was to build an innovative browser-based platform that would leverage advances in Web and security technologies to provide corporate treasury and investment professionals with integrated Internet access to their account information. In addition, customers would be given the ability to conduct a full range of financial transactions from a single application.

Solution

The bank chose Entrust Technologies to provide the public-key infrastructure necessary to create and deploy digital certificates to customers. After evaluating a number of Entrust-Ready™ products to create a Virtual Private Network (VPN), KyberPASS™ was the VPN product that passed the critical review.



Advantages and Benefits

In November 1997, the bank unveiled the first release of their integrated Web-based platform. The integration of KyberPASS family of products provided the bank's customers with a simple and transparent mechanism to leverage the Entrust public-key infrastructure and provide the necessary network security. The combination of Entrust and KyberPASS provided the Web-based platform with security features of strong identification and authentication of users, the establishment of secure encrypted sessions for ensuring privacy and data integrity, and audit logging to guarantee non-repudiation of transactions.

The Web-based platform “gives our customers a single, integrated point of access to their accounts and our products,” said a Services Executive representative. With the rollout of this platform, “we are the first bank to use Web-enabled technology for an information reporting and transaction initiation system.”

“We see tremendous growth of browser-based electronic commerce solutions and believe [the organization] is uniquely positioned to be a leading provider of these value-added services,” said one Client Access Executive. “With our integrated platform, we are setting the stage to deliver even more advanced services going forward.”

Entrust Helps Bank of Bermuda Become First International Bank to Run Its Own CA

ORGANIZATION

The Bank of Bermuda Limited

Industry

International and offshore financial services

CHALLENGE

To provide clients with secure and easy access to full banking and financial services over public networks

SOLUTION

Entrust Technologies —
Entrust/Direct™
Entrust/ICE™
Entrust/Entelligence™
Entrust/Web Connector™
Cisco PIX Firewall

RESULTS

- The only international bank that can offer multi-currency electronic commerce processing offshore
- Makes the bank more accessible regardless of the user's geographical location
- Provides more secure and better online service
- Optimizes client revenue, profitability and investments

Geography has never proved to be a barrier for the Bank of Bermuda.

Recognized as one of the world's leading offshore financial services groups and Bermuda's largest indigenous company, the 110-year-old bank claims corporate and private clients across the planet.

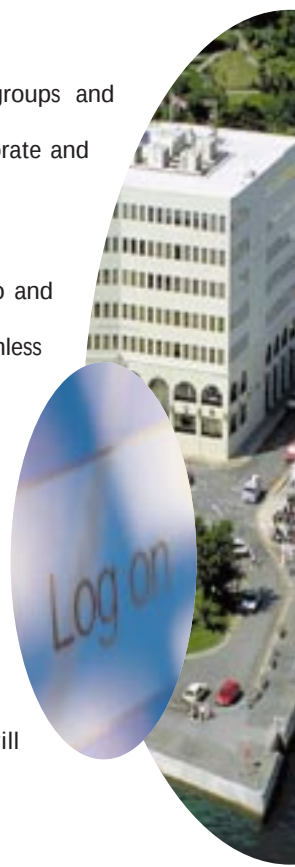
Situated no more than two hours away by air from New York and Toronto and boasting a year-round subtropical climate, the island in the Atlantic is a painless place to visit for those wishing to do their banking in-branch.

But the Bank of Bermuda didn't acquire \$10 billion U.S. in assets by touting the country's tourism alone. Indeed, Bermuda itself is on the road to becoming one of the world's most business-technologically-friendly countries through legislation supporting electronic commerce.

So too is the Bank of Bermuda undergoing significant changes that will further expand the manner in which its customers do business.

Virtual Banking

Currently, the bank supports a service whereby customers can access their portfolios, transfer funds or process credit card transactions electronically via a global private corporate network built around Cisco's secure PIX Firewall technology. With it, all you need to do is dial-up access through one of the Bank's 14 offices around the world.



But while clients have had a secure alternative for conducting financial and business transactions – an essential requirement by their and the Bank's risk-averse standards – not all have been keen on racking up long-distance charges every time they want to make a remote connection with the Bank.

So, rather than forcing the client in South Africa to dial up London thousands of kilometers away to get access to it, the Bank of Bermuda has, by tapping into the powers of public networks, come to the client.

Using public-key infrastructure technology provided by Entrust Technologies, the Bank has made its services available through the unsurpassed global reach of the Equant network, which extends to key business centers in over 220 countries and territories. Equant provides mission-critical solutions and has established itself as a leading provider of managed data network services, end-to-end, for multinational businesses worldwide, and provides Global Dial, PPP Dial, X.28, and Remote LAN Access Services to the Bank of Bermuda.

"We needed to be able to provide online access for our clients anywhere in the world to their portfolios electronically and be confident it was secure and encrypted," explains Gavin Grounds, assistant vice-president of global internetworking at the Bank of Bermuda.

"We also needed the ability to encrypt and digitally sign messages, files and file attachments."

"While other companies were capable of outfitting the Bank as a certificate authority to manage and issue digital certificates to clients and partners for conducting electronic business, none, save Entrust, were able to equip the bank with a one-stop shop."

One-stop Banking

He says the Bank chose Entrust solutions for the service called Secure Client Access because it offered a complete end-to-end solution.

“While other companies were capable of outfitting the Bank as a certificate authority to manage and issue digital certificates to clients and partners for conducting electronic business, none, save Entrust, were able to equip the bank with a one-stop shop,” says Mr. Grounds.

“When it came to the actual applications, such as sending encrypted e-mail, we would have been sent to a third party to provide that piece of software,” he explains. “Entrust allows us to use a variety of applications with a standard and consistent high level of security.”

As a result, the Bank of Bermuda can now provide authentication and encryption for online access to and management of portfolios, as well as support the digitally signing and encrypting of e-mail and file transfers into and out of the Bank.

Furthermore, the Bank can authenticate customers using its cash management, client-server software application, Bankline II, and establish an encrypted connection over the virtual private network linking the customer's PC and the Bank's server. This application allows clients to feed transaction instructions directly to the Bank's main banking applications.

“By introducing and implementing the Entrust-based solution, the Bank has positioned itself extremely well for enhancing its international e-commerce products offering.”

Bank of Bermuda's roll-out strategy has been to initially implement it internally, on a global basis, through departments responsible for corporate trusts, portfolio management and human resources, as well as a few pilot external users. Next, based on client demand, it will be further rolled out to external clients and will eventually involve some 10,000 users worldwide. This will further entrench the financial institution as the world's first international bank to build and operate its own private certification authority for internal and external communications.

Better Banking in Bermuda

Augmenting its user-friendly technology that is giving clients closer (and secure) access to it and its service offerings, the Bank of Bermuda, by virtue of its location, is providing customers with added value.

By enacting e-commerce-friendly legislation that legally recognizes digital signatures, Bermuda has made it even easier for the Bank's clientele to conduct business in a virtual environment.

The combination of technology and legislation also means the Bank of Bermuda's long tradition of being a global, and sometimes faraway financial player, now accommodates more of a community presence.

"Our clients in North America are more likely to work with Bank of Bermuda because we look and feel like we're just down the street."

Large Computer Manufacturer Paves the Way to the “Security Assured Organization”

ORGANIZATION

Fortune Global 100 Computer Manufacturer

INDUSTRY

Manufacturing - Hardware and software developer

CHALLENGE

To implement an overall security layer for the entire enterprise and for the 80,000 employees in various international locations.

SOLUTION

Entrust Technologies Inc. —
Entrust/PKI™
Entrust/Express™
Entrust/ICE™
Entrust/TrueDelete™

RESULTS

A complete solution that encrypts and decrypts files and data, verifies the identities of people communicating, and denies access to unauthorized individuals. Policies and procedures that would ensure that the technology would easily integrate into an organization moving at a high rate of speed every day.

As one of the largest computer manufacturers in the world, the company understands the importance of protecting IT investments. The personal computer has become a cornerstone of the information age, the holder of business-critical information from intellectual property to business contracts, the starting point for transactions and communications among employees, customers, and suppliers.

To protect that sensitive information, the company has pioneered a new approach to security, establishing a comprehensive infrastructure that includes policies and technologies, calling this approach the “Security Assured Organization”. Entrust Technologies, chosen as the security foundation by the company, is the worldwide market and technology leader in digital certificate and public-key infrastructures (PKIs). Entrust® solutions will secure some 80,000 of the company’s employees — their personal computers, laptops, and systems.

Business Situation

As one of the companies that created the computer revolution, the company understands the power of personal computing. But with desktop and laptop computers containing some of the company’s most sensitive documents — product plans, business contracts, sales figures — they also understood the need to protect those electronic assets.



Employees conduct 80% of computer system break-ins — it's the hackers who are responsible for the other 20% and get the publicity. The company recognized that security needs to control internal and external access — that firewalls need to be complemented by secure screen savers or passwords that protect information when employees roam away from their desktop or laptop computers.

The company also recognized that security needed to extend to employees working remotely. Sensitive data was coming in electronically to headquarters from employees working off-site. Contracts, product design specifications, and financial information were arriving via e-mail without any protection from prying, unauthorized eyes.

Business Goal — “Security Assured Organization”

What the company sought was an overall security layer for the entire enterprise and for the 80,000 employees in various international locations. The security layer had to include technology that encrypted and decrypted files and data, verified the identities of people communicating, and denies access to unauthorized individuals. That layer also had to include policies and procedures that would ensure that the technology would easily integrate into an organization moving at a high rate of speed every day.

The company sought to create a “Security Assured Organization” using Entrust solutions, in which policies, practices, and technology combine to enable an enterprise to take advantage of absolute security for all electronic transactions, files, and communications. While many corporations are discussing the creation of this tamper-proof environment, this company is among the first to take sizable steps toward this goal.

The company sought to create a “Security Assured Organization” using Entrust solutions, in which policies, practices, and technology combine to enable an enterprise to take advantage of absolute security for all electronic transactions, files, and communications.

As a Security Assured Organization, the company will be able to rely more on electronic methods to better integrate suppliers and customers, as well as its far-flung employees. Time to decision and market responsiveness can dramatically rise and paperwork loads can disappear as contracts move and are signed electronically; pricing requests can be acted upon immediately; and sensitive documents can flow over the Internet — safe from unauthorized access.

The Solution is Chosen

After a rigorous analysis of over a dozen security products, the company chose Entrust Technologies in October 1996 as the security technology of choice. Entrust's pioneering of public-key infrastructure (PKI), provides a single security foundation, and the mechanism to administer other Entrust security solutions.

Through the PKI, Entrust Technologies enables an organization to issue and manage digital certificates — the electronic equivalent of a passport — and encryption keys. Digital certificates and encryption keys protect many types of critical applications, from e-mail to e-commerce transactions and beyond.

Deployment Details and Business Benefits

As is typical in many large corporations, a project, especially an ambitious project to “securitize” over 80,000 employees spread over many continents, requires strategic and careful planning.

The company's security department set the groundwork for corporate-wide security policies. The company created a security hierarchy that details policies, standards and procedures around what will be secured, which Entrust products to use and when, and which employees will have access to what data.

The human resources group at the company created two classifications of data. Depending on the criteria for sensitivity, encryption was either mandatory or highly recommended but optional.

“With a good foundation, everything else falls in place,” said a company representative. “Without these policies written and accessible to the users, the program isn’t effective.”

To test the practices, policies, and technology, the company conducted a 100-employee pilot program, including engineers, administrators and other non-technical employees. The group tested secure e-mails and secure files across various hardware platforms and operating systems.

Not surprising, given how much communication is done via e-mail, the employees were enthusiastic about secure e-mail and having their desktops secure. Testing also proved that Entrust’s technology had only a minimal effect on network performance.

The company also developed an education awareness program to teach employees and remote access users the security policies, the technology, and the business advantage of using encryption.



Mackenzie Financial Corporation Gives Financial Advisors Secure Web-based Access to Accounts, Investment Portfolios

ORGANIZATION

Mackenzie Financial Corporation

INDUSTRY

Mutual fund, trust and investment services

CHALLENGE

To provide a secure and seamless system for financial advisors to access client information over the Web, improving service to advisors and investors while reducing costs

SOLUTION

Entrust Technologies —
Entrust/PKI™
Entrust/Direct™
PeerLogic i.500 directory
EXOCOM Technology
Solutions Corp.

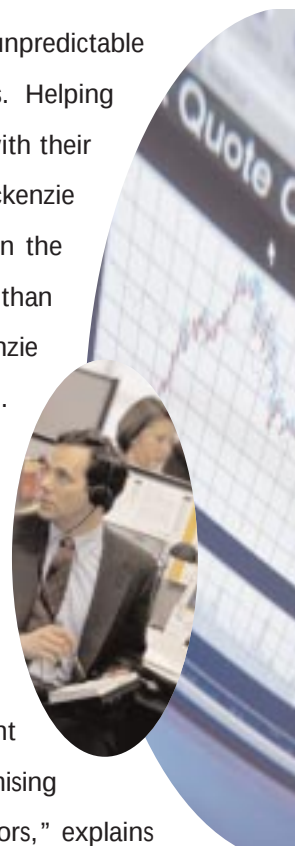
RESULTS

- Mackenzie Financial's Mackenzie AccessNet and MRS Symon financial advisor sites allow management of accounts and investment portfolios securely over the Internet.
- Mackenzie is now a certification authority that relies on a unique certificate registration process that streamlines the authentication of advisors and allows them to register for their security certificate online.

Within the competitive, fluid and often unpredictable marketplace, today's financial advice quickly becomes yesterday's. Helping Canadians to build financial independence by staying a step ahead with their mutual fund, trust and investment strategies is Toronto-based Mackenzie Financial's business which has helped make the company a leader in the Canadian mutual fund industry. Maintaining contact with more than 30,000 independent financial advisors that represent both Mackenzie Financial as well as its wholly-owned subsidiaries MRS Trust, MRS Inc. and MRS Security Services Inc., is a vital component in meeting that client-focused objective. This is especially true when dealing with rapidly changing investment markets, where information must not only be kept confidential, but must also be accurate and timely.

Like many major companies today, Mackenzie Financial has turned to the Internet as a way of connecting with the vast array of independent financial advisors. "We needed to ensure we did so without compromising the existing relationship of trust between the company and its advisors," explains Jim Haw, Vice-president of System Security and Standards for Mackenzie.

"At the very outset, when we considered extending the relationship with our financial advisors to the Web, we were insistent that proper security be in place first, before any client information was transmitted," he says. "Our business is built on trust. To expand the services we offer through the Web, our security solution had to provide positive, two-way authentication and the confidentiality of unit-holder information had to be protected at all times."



After investigating security products available in the marketplace, Mackenzie Financial assembled a solution the company feels meets its needs in providing both authentication and encryption, and which has made Mackenzie the first Canadian mutual fund services company to implement a strategic secure Internet-based business solution through its Mackenzie AccessNet and MRS Symon financial advisor sites.

EXOCOM, Entrust Partnership

In addition to the provision of the appropriate Entrust® and PeerLogic i500 product solution, end-to-end information technology security specialists EXOCOM Technology Solutions Corp. developed the security component for dealer registration, including the design of a front-end GUI. Through it, financial advisors complete an application, which is stored in a separate branch of Mackenzie's i.500 directory pending validation by the dealer services groups at Mackenzie and/or MRS. Mackenzie addressed the potential authorization obstacles of issuing certificates to advisors who could be affiliated with both or either organization through use of a single registration step and multiple workflows to pass the information through different validation and approval functions.

Once validated and approved, the applicant data is moved into the appropriate branch of the directory, a digital certificate is issued by Mackenzie's security group and an authorization code is forwarded to the applicant by e-mail. A reference code is returned to the dealer services group and confirmed by telephone with the applicant.

“Our partnership using Entrust solutions gives us a sound foundation upon which to build future applications over the Web. This combination of technical expertise and advanced technology equips us with a robust mechanism for establishing a trusted Web-based relationship with our business partners, and provides a solid base for added functionality in the future.”

Jim Haw

Vice-President, System Security & Standards

Mackenzie Financial

“Utilizing Entrust/PKI™ gives Mackenzie what we believe to be the best technology to meet our security objectives both now and in the future, while EXOCOM has delivered a solution that enhances the efficiency of implementing and maintaining the Entrust product,” Mr. Haw explains.

Unique Certificate Registration

Mackenzie’s infrastructure gives financial advisors the freedom and flexibility to manage accounts and investment portfolios securely over the Web. A key element of this infrastructure was the implementation of the unique certificate registration process described above. As a result, users have transparent and secure access while Mackenzie enjoys efficiencies and control over the issuance and management of certificates.

The Mackenzie AccessNet and MRS Symon sites rely on the Web to provide client information to brokers, dealers and financial advisors, allowing them to enquire against customer holdings, establish new accounts or modify client information, such as addresses and phone numbers.

In the future, both applications may be used to complement and supplement the functionality available through FundSERV Inc. — a private network between dealers and fund companies — currently used to process transactions against funds.

Thus far, 1,700 certificates have been issued and Mackenzie plans to expand that base to 5,000. Once fully implemented, the system could accommodate all of Mackenzie's financial advisors.

In the longer term, the company's secure presence on the Web could also facilitate access for some of Mackenzie's 1.6 million unit holders who could access Mackenzie via the Web to view account information, obtain confirmation of financial transactions and customer statements; this improves service and reduces costs while providing customers with all the benefits of working with a financial advisor in establishing and carrying through with their financial plans.

"Our partnership using Entrust solutions gives us a sound foundation upon which to build future applications over the Web," says Mr. Haw.

"This combination of technical expertise and advanced technology equips us with a robust mechanism for establishing a trusted Web-based relationship with our business partners, and provides a solid base for added functionality in the future."



NetEx Marks the Spot for Secure Document Transmission over the Net

ORGANIZATION

NetEx, Inc.
www.netex.com

INDUSTRY

Internet services

CHALLENGE

To create an easy-to-use transparent document management platform that features high-end security.

SOLUTION

Entrust Technologies Inc. —
Entrust/PKI™
EntrustFile Toolkit™
EntrustSession Toolkit™
Entrust/Toolkit Java Edition™

RESULTS

- A unique document delivery service on the Internet that provides high-end encryption with automatic digital certificate management on the both the Web and the desktop.

Guaranteed communication, on-time delivery and cost effectiveness are among the most important bottom-line considerations for business today. In combining these standards in their company's flagship product, along with the security features of Entrust®, NetEx, Inc. of New Orleans has a marketplace winner with a unique solution.

The NetEx software is a powerful combination of patented imaging technology and a Windows-based graphical user interface. The software provides a single, logical method of creating, sending and receiving all types of documents and e-mail over the Internet. NetEx interacts with a user's default e-mail system that allows the creation, transmission and receipt of all e-mail using an existing mail address book in one program — including Lotus Notes®, Microsoft Outlook®, and Microsoft® Exchange.

NetEx is designed for secure electronic transmission of any document, including those that are hand-written, paper-based, or that feature graphical images or electronic media. NetEx is also the first electronic-delivery messenger to automate the use of digital certificates for robust encryption and authentication of users' identities.

How it Works

A package is easily created by either attaching an electronic file, or by scanning a hard copy, or printing directly to the NetEx virtual printer driver. Once the package is



created, the NetEx software, which is free to use, secures and sends the encrypted package directly to the NetEx server. The server then processes the encryption, certificate security, authentication, tracking, confirmation and the archiving of all documents.

NetEx informs the recipient via e-mail, fax, pager or voice that a document has been sent to NetEx and is awaiting pickup. The recipient then accesses the NetEx server using a personal digital certificate for authentication, and downloads the package where it is automatically decrypted and opened.

“What’s exclusive to us is that you have the option of downloading, viewing a file and having it re-encrypted when you close the document where it remains in your hard drive,” says Greg Meffert, NetEx President and Chief Technology Officer.

“If I’m in the middle of an airport or at a client site and need to get at a document, I can download it. But even if a connection is secure, once a file is downloaded it’s wide open. But in this case, it stays encrypted and locked up on the hard drive.”

Encrypted and Economical

Using Entrust Technologies’ PKI solutions for e-business, Mr. Meffert says that NetEx is able to launch a new line of business that allows customers to save up to 80% over traditional express-delivery costs while preserving an environment with a high level of trust and document security.

Using Entrust Technologies’ PKI solutions for e-business, NetEx is able to launch a new line of business that allows customers to save up to 80% over traditional express-delivery costs while preserving an environment with a high level of trust and document security.

Greg Meffert

President and Chief Technology Officer

NetEx, Inc.

“Within the overnight courier market, which is approximately \$35 billion U.S. a year just among the major top-tiers, 30% of that business will belong to the Net,” explains Mr. Meffert.

With NetEx’s offering, the Internet could capture more of that market and realize “immediate cost savings” for major companies that typically ship paper documents in an envelope by messenger, he says.

Recently, Universal Express, Inc. of Plainview, New York announced that its Postal Business Center Network plans to use NetEx’s secure electronic delivery system for member stores.

To illustrate the cost-effectiveness of its solution, NetEx charges customers only \$9.95 a month to send between one and five megabytes of information (or between 30 and 150 pages of plaintext) through its secure transmission pipeline. That amounts to a \$27 savings over sending the same information by overnight delivery.

Entrust ‘Cream of the Crop’

Beyond the economics, security is vital to NetEx’s success, says Mr. Meffert, who explains that the firm shopped around before discovering the right combination that wasn’t “a hodgepodge of various technologies that wouldn’t have worked as well.”

As he explains, “There’s a perception in the marketplace – an accurate one – that Entrust encryption technology is the cream of the crop.”

NetEx uses Entrust Technologies’ flagship software, Entrust/PKI, to issue and manage digital certificates that provide full-strength encryption to protect sensitive documents, and authenticate senders and receivers so only trusted receivers are able to unscramble the message.

“We are the document delivery service on the Internet that provides high-end encryption with automatic digital certificate management on both the Web and the desktop,” Mr. Meffert says.

“There is nobody that is offering the level of security that we’re offering. Every competitor we have offers security in the transmission of the document, but does not offer security after reception.”

He adds that NetEx is able to control whether a document is forwarded, or allows a user to forward a file and obtain confirmation as to the document’s destination path.

“The challenge for us was to create a platform feature-rich enough, and transparent enough to the user in an easy-to-use interface that features high-end security. Only this way can we present a viable alternative to the existing mode of document management,” Mr. Meffert says.

PKI Gives Secure Point-to-point Delivery

With Entrust Technologies’ public-key encryption technology, NetEx is in a position to offer customers a “plug-and-play, one-stop shop for the point-to-point sending of messages and documents,” Mr. Meffert explains.

By mid-2000, NetEx expects that its secure transmission product will be available to “hundreds of thousands” of customers.

NetEx itself has found using its all-in-one secure electronic transmission software invaluable in the way the private firm runs its own business, says Mr. Meffert. “In one of our investment rounds, we closed a deal on NetEx.”

PKI provides security and efficiency to New York Life

ORGANIZATION

New York Life Insurance Company
Industry
Insurance and financial services

CHALLENGE

To provide a secure and cost-effective online network for agents and brokers to access client files and policy information

SOLUTION

Ifsec, LLC
Entrust Technologies Inc. —
Entrust/PKI™
Entrust/Direct™
Entrust/Entelligence™

RESULTS

- Online access for field agents and office employees that encrypts files and sessions, and authenticates users
- Quicker turnaround time
- Less than half the cost per month to maintain the previous system

With \$80 billion U.S. in assets and three million policyholders, New York Life has a lot of information to manage. Having convenient access to client files has been a challenge for the company's agents and brokers who spend considerable time away from their offices.

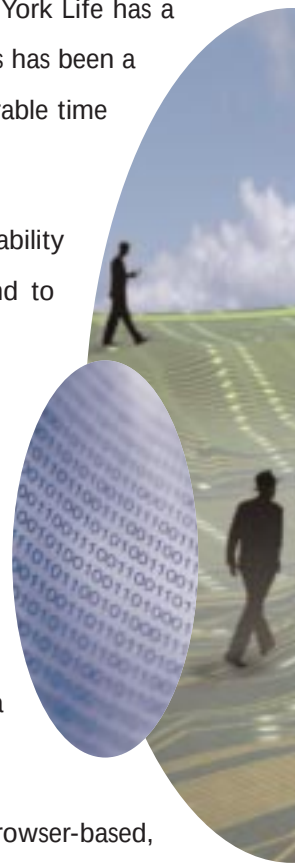
Last year, the New York-based, Fortune 100 company enhanced its ability to offer agents and brokers access to client policy information, and to download change-of-address and beneficiary forms for customers.

The decision to implement Entrust Technologies' public-key infrastructure solution was in part based on improving the manner in which agents and employees could access client files and policy details, says New York Life Vice-President Steve Attias.

"We wanted to allow our field agents to request policy information and have access to critical resources that they otherwise couldn't in a timely manner using other means."

New York Life also wanted a desktop application that would be browser-based, providing access to as many employees as possible.

"Most importantly, we were looking for a modular solution adaptable enough that would allow us to add new applications as they arose," explains Mr. Attias.



Life Before PKI

Prior to considering a PKI, New York Life was using a mail-enabled, value added network (VAN) based application that gave agents access to sensitive information. Agents would dial directly into proprietary access points of presence (POPs). A custom-built application allowed agents to enter a formatted request by e-mail, which was then forwarded to New York Life's systems, processed and returned to them by e-mail.

While the system bore encrypted-security features, information requests experienced slow turnaround times. This electronic pipeline also proved to be expensive – nearly \$500,000 U.S. a month.

In addition to its mail-enabled application, New York Life also deployed a Web application that provided access for field agents and office employees to control encryption and fire-walling functions in a single module. Unfortunately, it didn't allow the company to replace individual components with better ones and did not provide flexibility needed to support the security administration over a large population.

Most importantly, the company needed to find a way to provide secure authentication and encryption to protect the integrity of sensitive client information over the Net while giving field agents secure access to it.

“We now can offer real-time access to information over the Web and have the confidence that the information the agents receive isn't compromised.”

Steve Attias

Vice-President

New York Life Insurance

The All-in-one, Low-cost Solution

With Entrust Technologies' PKI solution, New York Life found the right mix that allowed the company to create a Web-based solution which could provide secure communications and strong authentication of users between its agents, brokers, and employees. It has also proved to be a cost-effective choice, helping New York Life save over \$200,000 U.S. in monthly costs, and allowing the company to recoup the costs of implementing the PKI in less than 12 months.

The first phase of the PKI rollout involved New York Life's 8,000 field agents — half of which were on board by the end of last year or six months after initial deployment.

The second phase is intended to provide certificates to New York Life employees so they can access secured applications and reduce the impact of multiple sign-ons to different applications.

"We now can offer real-time access to information over the Web and have the confidence that the information the agents receive isn't compromised," Mr. Attias explains.

"Our use of Entrust Technologies' flexible e-based solutions will support the change in our communications methods, result in cost savings for the company and will ultimately benefit our customers through improved agent productivity and service."



**Enabling trusted e-business
transactions over wireless
networks and the Web.**

Lower costs and offer new services

Entrust.net solutions include Web and wireless
server certificates and innovative management
tools to help you lower costs and manage trusted
e-business transactions between your customers,
partners and employees.

Find out more

**Visit www.entrust.net or
call 1-877-ENT-SITE**

We Bring Trust to e-Business™

North Dakota Secures State Information

ORGANIZATION

State of North Dakota
Industry
State government

CHALLENGE

To facilitate secure access for state employees to access computerized information throughout North Dakota's government in a controlled and secure environment.

SOLUTION

Entrust Technologies —
Entrust/Direct™
Entrust/Express™

RESULTS

- Authentication of Web-based transactions accessing confidential information
- Secure internal e-mail system for state employees
- Secure environment for mainframe access

Over the past few years, the federal and state governments in the United States have been looking for ways to make the Internet a safer and more secure electronic hub for the exchange of information.

In the process, lawmakers in Washington, D.C. have established frameworks and guidelines facilitating Web-based electronic commerce, as well as the sharing of personal information that respect privacy and confidentiality. In North Dakota, legislation empowered the Information Technology Department to “address the deployment of encryption and the administration of digital signatures.”

Both results are of key importance to the State of North Dakota, which established a digital encryption committee composed of telecommunications, security and computer systems specialists with the goal of creating a secure environment in which employees could exchange electronic information.

Initially, the committee was looking for a Web-authentication solution, until continued encryption research exposed the group to Entrust Technologies, says Dean Glatt, Associate Director of the North Dakota Information Technology Department.

“We found that Entrust's suite of products addressed various needs – not only our encryption requirements, but our need to have a public-key infrastructure that our security personnel can control.”

The State of North Dakota has chosen to deploy Entrust® software solutions to create a secure environment for state employees to access data.

Mr. Glatt says that the Entrust solution will allow the state government to build on future requirements, such as VPNs, TN3270 and TN5250 encryption to ensure the continued protection of data.



“We selected Entrust/PKI™ based on the strength of its ability to support centrally managed keys,” he adds. “When investigating the marketplace, we found Entrust Technologies was the only vendor able to provide us with the right technology in a configuration we needed.”

The State of North Dakota is using the advanced Entrust model for Web security, Entrust/Direct™, for trusted authentication of applications.

Entrust/Direct replaces existing security functions in Web-based applications with the scalable enterprise security of Entrust/PKI, allowing for a further level of integration with Entrust's flagship software.

The state will also use Entrust/Express™ for Microsoft Exchange and Outlook for trusted internal e-mail communications.

Mr. Glatt says that it is possible that the Entrust suite of products can provide data integrity for all areas of data on his department's networks.

“The beauty of the system is its invisible deployment for the end users,” he explains.

This centralized, cost-effective and secure electronic environment for data access began with a pilot in June and North Dakota's Information Technology Department expects to have hundreds of employees use the system for Web and e-mail authentication and encryption.

“Employees who have used it so far don't even know that authentication, encryption and messaging integrity is occurring. Furthermore, they don't need to have technical expertise to use encryption and key management. It happens automatically and transparently,” Mr. Glatt explains.

“Users should know data is being used and processed in a secure, confidential and private way. The security standards that we are developing will maintain the highest security of all electronic information.”

“We selected Entrust/PKI based on the strength of its ability to support centrally managed keys,” he adds. “When investigating the marketplace, we found Entrust Technologies was the only vendor able to provide us with the right technology in a configuration we needed.”

Perot Systems' VPN Increases Access, Cuts Costs

ORGANIZATION

Perot Systems® Corporation
<http://www.perot.com/>

INDUSTRY

Systems integration and consulting

CHALLENGE

To provide a cost-effective, secure and reliable network in which employees can access client files from remote locations and customers can access applications.

SOLUTION

Entrust Technologies —
 Entrust/PKI™
 Check Point™ – VPN-1
 SecuRemote
 Novell® NDS
 Cisco® routers

RESULTS

- Secure online entry point into the company
- Employee access to client files and customer access to applications in a shared environment

Like all large organizations today, Perot Systems' success lies in maintaining a sound and solid information network with its employees and clients. By building a system that both supports close relationships and is cost-effective, the Richardson, Texas-based IT services company, founded by former U.S. presidential candidate Ross Perot, has secured a competitive edge in the marketplace.

Perot Systems' solution lies in transferring the company's back-end applications from private-leased lines onto the Internet using virtual private network technologies over the next five years.

By embracing VPN technology, Perot Systems plans to move its corporate systems and standard Web and e-mail applications from frame-relay running on leased lines to the Internet.

The company is among many that have turned to VPNs to facilitate remote employee access to corporate data, reduce costs associated with maintaining clunky legacy networks, and forge new relationships with customers and suppliers over the Internet.

Mission-Critical

Should Internet service providers provide strong assurances for reliable connections and speed, VPNs could soon fill the role as full mission-critical enterprise networks. Infonetics Research Inc. of San Jose, California, predicts global spending for VPN services, hardware and software will climb from \$2.4 billion U.S. to \$32 billion U.S. by 2003.



Furthermore, a recent survey of 50 IT managers conducted by Forrester Research Inc. of Cambridge, Massachusetts found that 62 per cent had a VPN in use or in the pilot stage; 30 per cent planned to use a VPN within two years.

For its part, Perot Systems is building server-to-server VPN connectivity between 20 remote domestic and international sites and Perot Systems' corporate network in Plano, Texas. The VPN infrastructure will be deployed over the next year. When it is completed, the network will help cut costs.

Faster, Cheaper

Previously, Perot Systems' frame-relay connection, at a speed of 128-Kbps, would cost \$1,140 U.S. per month to maintain.

Now, with a T-1 connection whizzing at a speed of 1.54-Mbps, the cost will be nearly half at \$600 U.S. a month.

And rather than having to make endless and expensive long-distance calls to access client files at Perot Systems' data center in Richardson, the company's global workforce of over 6,000 employees – many of whom are based at client sites – will be able to access the information quickly and affordably over the Internet.

Perot Systems' customers also benefit by now being able to access applications, such as customer service, in which they can check the status of requests, make amendments or add comments online.

"If you don't play on the Internet, you're not going to play long," says Richard Karon, Perot Systems' Network Security Business Developer in Plano, Texas.

Working with several partners to build its VPN, Perot Systems plans on setting the standard for VPNs, eventually offering solutions based on the technology to its Fortune 500 customers.

Entrust provides authentication and transparent key management. Currently, every Perot Systems VPN user is assigned a security policy, which outlines the parameters of that individual's access within the company's network.

"Entrust's technology represents a fundamental aspect of our VPN. The company is the premier supplier for PKI technology and Entrust's certificates give us the ability to provide the kind of security we were looking for – a mechanism for strong authentication – as well as the scalability we need."

Richard Karon

Perot Systems

Network Security Business Developer

Mobile employees' laptops are equipped with VPN-1 SecuRemote client VPN software from Redwood City, California-based Check Point Software Technologies Ltd.

The software enables remote client users to access the corporate network through dial-up Internet connections and establish secure VPN sessions.

Check Point's VPN-1 products establish secure communication channels with users at Perot Systems' remote offices using certificate-based authentication from Entrust® Technologies' managed PKI solutions. This ensures that only authorized users have permission to handle client files in the data center, access PeopleSoft Inc.'s financial and human resources applications, and use IT help desk and ticketing applications. Entrust/PKI manages the generation, signing and revocation of X.509 certificates, and performs transparent key and certificate management for end users – all of which are necessary to provide the scalable trust necessary for large-scale VPNs. Perot Systems' business customers will eventually access applications and information in the same manner.

Among the applications being accessed is time tracking for consultants. Eventually, authorized Perot Systems VPN users will be able to send and receive secure e-mail.

As well, Perot Systems is rolling out Cisco routers for site-to-site remote office VPN that encompasses Entrust/VPNConnector™ to ensure authentication and authorization with a remote office.

"Entrust's technology represents a fundamental aspect of our VPN," Mr. Karon explains.

"The company is the premier supplier for PKI technology and Entrust's certificates give us the ability to provide the kind of security we were looking for – a mechanism for strong authentication – as well as the scalability we need."

He says that Entrust Technologies provided Perot Systems with "Cadillac service that dealt with our issues and challenges professionally and efficiently."

Mr. Karon adds: "Our VPN is fundamental to our business and too important to relegate to a third-party service provider to maintain. The decision to maintain the operation of this system was only reinforced by our partnership with the solid technology and approach Entrust offers us."



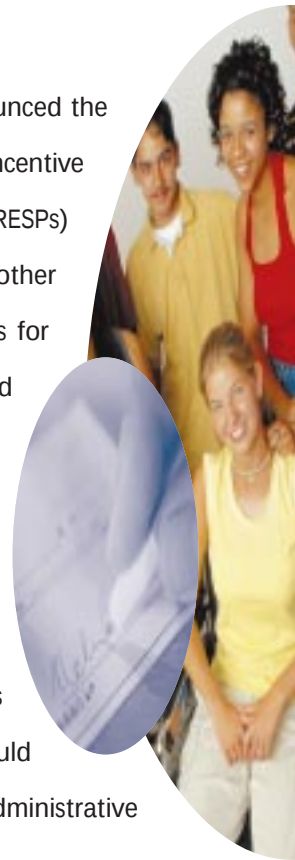
Federal Government Implements the Canadian Education Savings Grant with Help from ViaSafe® and Entrust Technologies

In the Canadian Federal Budget of 1998, the Finance Minister announced the Canada Education Savings Grant (CESG). The CES grant provides an incentive for parents and others to save in registered education savings plans (RESPs) for the post-secondary education needs of their children and other beneficiaries. A CES grant of 20% is paid on contributions to RESPs for eligible beneficiaries, up to an annual maximum of \$400 Cdn. and a lifetime maximum of \$7,200 Cdn. Human Resources Development Canada (HRDC), which administers the grant, made the first CES grant payments to trustees of RESPs in November 1998.

At the time of the CESG introduction, the existing reporting mechanisms for financial institutions to transmit information to the government could not adequately support the programs' specific technical and administrative requirements.

Challenges

To support the CESG, HRDC required a secure, manageable, cost-effective solution for sharing financial data between the department and RESP retailers. The Director for Systems Development of the CESG, Paul Jean, Jr., identified several strict business requirements including:



- Scalability to accommodate up to 200 RESP promoters and Grant trustees;
- Easy implementation and multiple platform support;
- Security for financial transactions between the promoters and trustees;
- Non-repudiation and authentication for transactions;
- Error tracking, transaction tracking and archiving; and
- End-to-end management.

Solution

HRDC chose a secure Internet-based solution because it is an accessible public network and electronic transactions can be easily secured using public-key cryptography. To help deliver the solution, the Government Telecommunications and Informatics Services (GTIS) recommended ViaSafe, Inc., a pioneer in secure electronic transactions, and Entrust Technologies, a leader in public-key infrastructure technology.

Despite very tight deadlines, the application was deployed quickly and satisfied the business requirements given:

1. Easy implementation. All RESP promoters have access to the Internet. Each user simply installs the ViaSafe Agent™ which ensures the transaction delivery and transaction receipts. HRDC enforces the rules to establish the business relationship — a process that can be accommodated within an hour.

The government benefits from a managed system that leverages the automated information integration strengths of ViaSafe and the security features of Entrust® in a seamless manner.

2. ViaSafe® software is Entrust-Ready™ and seamlessly leverages the security features of Entrust/PKI™ to ensure authentication of users, integrity of data and non-repudiation. ViaSafe implements a transport algorithm that guarantees delivery of secured data. ViaSafe can use Entrust's cryptographic technology to secure and authenticate data while in transit over the Internet. This way, digital certificates establish the credentials of parties and non-repudiation is ensured.
3. The solution did not require any alterations to the existing application - an important selling feature since RESP promoters had their IT resources otherwise committed to Y2K projects.
4. The system is scalable to accommodate the predicted growth of 200% in its first 12 months.

Results

The CESG Program has a secure and manageable system that fosters confidence in the parties it serves. The RESP promoters supply secured information knowing it will be tracked and administered quickly. The government benefits from a managed system that leverages the automated information integration strengths of ViaSafe and the security features of Entrust in a seamless manner. Further, all of this was possible without disrupting the older application that was in use. Therefore, the return on investment was immediate and users have a system that:

- Is flexible and can accommodate growth;
- Provides total non-repudiation using PKI keys;
- Encrypts transactions to ensure confidentiality; and
- Provides automatic transaction processing that led to an end-to-end Electronic Commerce Solution.

Using this system, the government can manage its program in a streamlined and highly dependable fashion and as a result, their financial institution clients are better served. This application illustrates the greater efficiency that can be achieved by deploying secured electronic applications that compliment each other, and the way organizations already do business.

The Treasury Board of Canada has noticed the success of the CESG system. The system was designated for Pathfinder Project as a model of electronic commerce in government. The Board has concluded that this project is highly suitable to be showcased in public as a leading PKI Pathfinder — to other departments and agencies, to other governments, at conferences and symposia, in promotional material, and so on. In addition, there is a promising potential for the model and practices to be used by other departments and agencies across government in their electronic commerce initiatives relating to use of the Internet, to the financial sector, and to establishing connections with partners outside government.