Date: Thursday, December 12, 1996

To: Mr. John Sheldon

From: Deepak Moorjani

Subject: Project Pak

Overview

Nortel is offering an equity interest in Entrust Technologies. Entrust provides a complete solution of encryption and authentication through various public key management systems. Entrust is in its final beta and will be released in late January.

Product

Entrust provides a comprehensive security product based on public key encryption. To date, there have been a number of security-related products (e.g. firewalls), but Nortel wants to distinguish itself by providing a full solution. Nortel has always had strong security products in the telco world (well-regarded X.25 security solutions) and can take advantage of its distribution capabilities.

Investment Rationale

Market: The opportunity is HUGE. As computers continue to get networked, security of information become important. Solving security issues will increase the types of applications that can be accessed through public networks. Major potential applications (e.g. Internet commerce) depend on this development.

Competition: Still in its infancy. While the Internet market has traditionally valued those that are first to market (e.g. Netscape), there will be opportunities for more than one company. The leading browser companies have decided to embed some security measures into their browsers.

Netscape has devised SSL (Secure Socket Layer), and this is backed by IBM and Microsoft. It is widely used (given the fact that it is embedded in the browser) but has been subject to some criticism (remember the famous Netscape security breach?). Microsoft is developing an SSL superset protocol called PCT (Private Communications Technology).

To date, the leading competition is from VeriSign (and its parent company - Security Dynamics. VeriSign just raised $30mm in a private offering, and the investor base included Comcast, Cisco, First Data, Gemplus Card (huge French smart card vendor), Intuit, Microsoft, Reuters, AT&T, and Softbank. These investors are expected to embed VeriSign's technology into their own products which implies that the company's products will be used Looks like a very tough competitor. They will also use the relationships of Security Dynamics

A strong valuation benchmark is Cylink which went public earlier this year. Cylink trades at 7.6x LTM revenues of $45.2mm (and implies a $108 valuation for Entrust).

Did I mention that the market opportunity is HUGE?

VeriSign

VeriSign's products secure electronic documents, financial transactions, and electronic mail transmitted over public and private computer networks. The VeriSign Digital ID technology will be embedded in a broad range of software products including operating systems for PCs and Internet server computers and enhances the security of encryption alone. The Digital ID which will provide users with a "driver's license for the Information Highway." Its technology will also serve as a link to VeriSign's authenticating service (Certification Authority), and VeriSign plans to license other companies to provide this service as well. VeriSign's business model assumes that any sort of transaction or security concern can be solved by having an independent CA, and VeriSign hopes to derive its revenue by serving as the CA.

Advantage Over VeriSign

Entrust will make its introduction into the security market in late January with Entrust/Web CA. It is a variation on Nortel's comprehensive Entrust security product line that extends the current Entrust CA to the Web. Corporations will be able to certify internal Web servers (either Microsoft's Internet Information Server or Netscape's Enterprise or FastTrack servers) and issue digital IDs through a Web front end to users of either Microsoft's Internet Explorer or Netscape's Navigator 3.0.

Entrust utilizes a different approach than VeriSign and allows anyone to be a Certification Authority. VeriSign and other public certification authorities (CAs) are necessary for public transactions between parties that do not know each other, but they are generally unnecessary for communicating within organizations or between closely cooperating companies. However, no matter what CA software is adopted, the upgrade path will be the most important consideration in selecting a vendor. Web-based encryption currently has several limitations, including the fact that keys that are created are not useful beyond the Web browser and server. For many companies, the Web will be the first exposure to the Internet and encryption and digital signatures can have wide application in simplifying access and data security throughout an organization. Entrust provides a full upgrade path.

Product Description

Entrust is a robust, fully standards-based system for managing keys in a large organization. Since it has been around since 1994 and fully implements the X.509 standard for key format, there are already many applications that now how to use the system making encryption and digital signatures as seamless as possible. Entrust provides a comprehensive public key management solution, and these solutions for LANs, WANs and public networks must perform each of the following five critical functions:

- Access Control - Access to a computer or network must be limited only to specific authorized users.
- Privacy - An unauthorized user must be prevented from viewing private data.
- Authentication - The receiver of the transmitted information must be able to verify the identity of the sender.
- Integrity - The receiver and sender must know that the transmitted data has not been changed or compromised by any unauthorized manipulation.

- Non-repudiation - Both the sender and receiver must be able to verify that a data transmission has been executed and cannot be later repudiated by either party.

To date, the demand for information security over public networks has been addressed by only partial solutions. "Firewall" products offer access control primarily by filtering incoming information based on packet addresses. Greater access control is possible with secret passwords of various types, including the use of time-varying and challenge-response password tokens. These tokens and access control systems generally provide some level of user authentication, but not privacy, integrity or non-repudiation. Many other encryption products provide privacy, but do not perform the other security functions and are not easily controlled or managed from one central location.

Market

Until 1993, sensitive data was primarily transmitted through private leased lines, but organizations are increasingly using public networks to transmit sensitive data and conduct transactions. When compared to private leased lines, public networks offer improved support at a lower price, primarily due to the economies of scale with large numbers of people sharing the network, and this has been an important factor that has led to the switch from private leased lines to public networks.

While public networks are becoming widely accepted, the shift is still in its early stage and security is a MAJOR concern for all end users. The Internet is estimated to have approximately 50 million users worldwide, and this number is increasing rapidly. Much of the recent growth of the Internet has been attributed to an increase in commercial organizations that seek to market products and services to users.

In public networks, sensitive information can be exposed to, viewed, manipulated and diverted. The desire of organizations to maximize the benefits of Internet and intranet connectivity, while limiting the related exposure of such information and applications, has created an increased demand for network security solutions. Major applications such as Internet commerce depend on it (e.g. if you send a credit card number over the Internet, how does the recipient know that it is really was you who placed the order?). These increasing levels of electronic commerce place a premium on ensuring the integrity and security of information transmission.

Security Market

The Yankee Group, a market research firm, expects the information security market to grow at a 70% compounded annual rate to the end of the decade from $395 million in 1995 to $5.6 billion in the year 2000. The forecasting model assumes the following: (i) the leading security vendors focus on educating end-users and resellers throughout 1996; (ii) the current pace of new product releases (2-3 per year) is maintained; (iii) standards are adopted and implemented by the beginning of 1997; (iv) the U.S. government allows the export of 64-bit keys by the middle of 1997; (v) foreign governments allow the use of strong encryption in their countries by the end of 1997.

Encryption Methodologies

Security products typically use one of two basic technologies: symmetric key or asymmetric key. Symmetric key systems rely on one password that the user must have in order to view information. This systems works fine when one can transmit the password to the person who will decode the document. If not, one must rely on a phone call or email message and hope that it remains confident.

Nortel uses public key (aka asymmetric) encryption. Asymmetric encryption uses two keys and solves the problem of providing a secure key to the user. To send a secure message, one uses the recipient's public key to encrypt the message, and the reader uses a private key to read it. While the two keys are complementary, it is nearly impossible to extract the private key from the public key.