MEMORANDUM GENERALE SOCIÉTÉ GÉNÉRALE

NEW YORK

TO: Distribution

FROM: David I. Brunson
Leveraged Finance

SUBJECT: ENTRUST TECHNOLOGIES INC.

DATE: December 18, 1996

This is to confirm that we will be meeting with the Company and their Advisor, DLJ, at 9:00 a.m., Thursday, December 19th, in the Conference Room on the 8th Floor. Attending from the Company will be:

John Ryan	Interim CEO & Director of the Company (and Vice President & General Manager, Multimedia and Internet Solutions of NTI)
Brian O'Higgins	Executive Vice President & Chief Technology Officer
Brad Ross	Executive Vice President, Marketing & Product Line Management

DLJ will be represented by Bob Diemar, Managing Director.

As background and supporting information, please find attached the Investment Committee memorandum and its exhibits.

There will not be a formal presentation as this is our meeting to conduct and pursue our diligence as we see fit. We have a number of questions and areas to pursue, thus, the meeting is expected to last 1-1 1/2 hours. Immediately afterwards, we will discuss the merits of this opportunity. If consent is achieved, we will seek to contact Curt in Paris.

Should you have any questions, please feel free to contact me.

David

DIB/is
attachment

Distribution:

Curt Welling
Bob Pirie
Greg Malcolm
Steve Baronoff
John Sheldon
Fiona Tilley
Deepak Moorjani
Jack Stack
Olivia Feldman

To: Distribution list
From: Deepak Moorjani

ENTRUST TECHNOLOGIES

Overview

Nortel is offering a 20% equity interest in Entrust Technologies and has approached SGIB (through DLJ) concerning a possible investment in the company. Entrust provides software products that address the growing need for security in electronic transmissions by providing encryption and authentication through its public key management system. Based on reviews, the Entrust product is the leader in standards-based, cross-platform public key certificate management for corporate use. DLJ has hard-circled $10 million from Olympus at a post-money valuation of $90 million and wants to close this round of financing by year-end. Nortel has always had strong security products in the telco world (well-regarded X.25 security solutions) and believes that it can use its experience and distribution capabilities to aid Entrust.

Product

Entrust is a family of public-key cryptography software products for encryption and digital signatures on computer networks with fully automated key management. Entrust offers encryption and digital signatures that offer solutions to the five fundamental network security requirements: confidentiality, access control, integrity, data origin authentication, and non-repudiation. Encryption addresses the confidentiality and access control requirements. Encryption can be used to make a file private so that only the people authorized can decrypt the file to read the information. Digital signature addresses the integrity, authentication, and non-repudiation requirements. A digital signature is analogous to a handwritten signature in that a digital signature can be used to assure a reader of the (non-repudiable) source of the information. In addition, a digital signature can ensure that any unauthorized changes to the data will be detected (integrity).

Public Keys

Keys are like passwords. The term key management refers to the secure administration of keys to provide them to users when and where they are required.

While it is safe to send encrypted messages without fear of interception (because an interceptor is unlikely to be able to decipher the message), there always remains the problem of how to securely transfer the key to the receivers of a message so that they can decrypt the message. Historically, encryption systems used what is known as symmetric cryptography. Symmetric cryptography uses the same key for both encryption and decryption. However, a major advance in cryptography occurred with the invention of public-key cryptography. The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption.

For example, if SocGen wants customers to be able to send it encrypted documents (perhaps to conduct transactions), SocGen and its customers probably do not want to utilize symmetric encryption because a password or key might be intercepted during transmission. Instead, SocGen can utilize public key (aka asymmetric) encryption. SocGen gives all of its customers the

SocGen public key. Customers then encrypt documents with SocGen's public key and sends these encrypted documents to SocGen. SocGen is then able to decrypt these documents with its private key, which is the only key that will decrypt these documents encrypted with SocGen's public key.

Whether or not anyone has SocGen's public key is irrelevant, because the public key is not able to decrypt documents. And the private key, which is known only to SocGen, does not have to be transmitted; theoretically, it never has to leave SocGen which means that the integrity of the key is never compromised. Conversely, some public-key cryptosystems allow customers to encrypt documents with their own private keys and then give their public keys to SocGen so SocGen can unencrypt the document.

Competitive Advantages: Scaleability/Public Key and Applicability beyond Web

Entrust is a unique product in a new product category known as Public-Key Infrastructures (PKI). The Entrust offering is unique in that it is scaleable and allows corporations the ability to extend this security beyond the Web.

Scaleability/Public Key: Most of the offerings from competitors are geared to individuals or small groups. The Entrust/Client application provides, using public-key cryptography, similar capabilities to these products but is supported by an automated key management infrastructure which scales to enterprise levels of tens of thousands of users and beyond. The Entrust solution ensures key updates are automatic, transparent to users and have no additional cost attached. This ensures that, as network security is deployed on a large scale, network administration costs are minimized, yet critical centralized controls are maintained.

Applicability beyond Web: Entrust will release Web CA in January. For many companies, the Web will be the first exposure to encryption and digital signatures; however, encryption and digital signatures have wide application throughout an organization (simplifying access and data security) and can provide benefits beyond the Web. Thus, the most important consideration for companies is to consider the upgrade path when choosing a CA, and Entrust is unique in that it offers a full upgrade path. Web-based encryption currently has many limitations including the fact that the keys that are created are not applicable beyond the Web browser and server. However, Entrust is competitive in that it is a robust, fully standards-based system for managing keys within a large organization and provides a full upgrade path. Since it has been around since 1994 and fully implements the X.509 standard for key format, there are a number of applications currently available that know how to use the system which makes the upgrade for encryption and digital signatures as seemless as possible.

Market

The market opportunity is HUGE. 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. As computers continue to get networked, security of information becomes extremely 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. 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 engage in electronic commerce (banking, trading securities, verifying credit and purchasing products and/or services).

Market Evolution

Until 1993, sensitive data was primarily transmitted through private leased lines, but the popularity of the Internet means that 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 achieved through larger 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. As organizations increasingly rely of the electronic transmission of data, their information becomes increasingly vulnerable. 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.

Competition

Competitors in this burgeoning field include a number of small startups including Cylink, V-One, and Axent Technologies. To date, the leading competor is VeriSign (a subsidiary of Security Dynamics). VeriSign just raised $30mm in a private offering from an investor base that includes 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 to guarantee that VeriSign's products will be used extensively.

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 will enhance 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 for a yearly fee.

Advantage Over VeriSign: Ability to Internally Manage Security

Entrust will make its introduction into the Web 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.

Entrust utilizes a different approach than VeriSign. VeriSign assumes that there is a need for an independent Certification Authority to facilitate security between parties and its system basically requires companies to outsource their security. While VeriSign and other public certification authorities may be most appropriate for public transactions between parties that do not know each other, one of the major benefits of the Internet is to spur disintermediation, and the VeriSign model is in stark contrast to this trend in that it involves an extra middleman. Entrust allows companies to bypass a public Certification Authority (CA) by allowing companies to be their own Certification Authority. This model is built on the fact that independent CAs are generally unnecessary for communicating within organizations or between closely cooperating companies. Additionally, companies may be very hesitant to give up direct contact with customers by involving a middleman.

Valuation

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). Additionally, V-One went public in October with a market capitalization of $61 million with 1996E sales to be $5-7 million. Entrust valuation (approximately 6x 1996 revenue) seems to be slightly lower than the public comps.

they confirmed our suspicion that many of customers will not adopt the verisign model, because they do not want to give up control of the customer. in a sense, verisign is asking its customers to outsource security, and no one wants to do this.

Due Diligence

I recently spoke with the V-One Corporation, another Internet security company. In general, they were complimentary about Entrust and said that Entrust is doing very well in the financial community (the ones that are in a position to drive electronic commerce). People like Entrust because it allows them to manage the certificates themselves. While the market in general is still up in the air, they say that the majority of the interest is in Entrust.

Their main concern was that, in a sense, Entrust is a bit proprietary in that customers need to rely on Entrust to manage the keys and for directory services. We should question management on this, but it is probably part of the management's desire to create an annuity stream from its product. In a sense, it makes them like a telco in that they own the dial tone of security.

On the competitive side, the real threat is from AT&T, Motorola and GTE. V-One does not really see Netscape/Microsoft as a real player because 1) they're version of security is web specific (the digital ID does not exist outside of the web) and 2) the browser authenticates the machine (and the ip address of the connection), not the user. And it is the user that needs to be authenticated.