Feltl and Company
SECURITIES BROKERAGE AND INVESTMENT BANKING

Jay M. Meier
jmmeier@feltl.com
(612) 492-8847

Security/Software
February 6, 2008

Entrust, Inc. (ENTU – $2.16)

Initiating coverage **STRONG BUY**

Financial Summary

Rev(mil)	2007A	2008E	2009E
Mar	$24.6	$26.3	
Jun	$24.5	$26.7	
Sep	$23.9	$26.6	
Dec	$26.7	$29.3	
FY	$99.7	$108.9	$121.3E
P/Sales	1.32x	1.21x	1.09x

PF EPS	2007A	2008E	2009E
Mar	($0.01)	$0.01	
Jun	($0.02)	$0.02	
Sep	$0.00	$0.03	
Dec	$0.04	$0.04	
FY	$0.01A	$0.11E	$0.17E
P/E	na	19.6x	12.7x

Price:	$2.16
52-Week Range:	$4.60 -$1.65
Target:	$4.50
Rating:	STR. BUY
Shares Outstanding:	61.1 mil
Mkt. Capitalization:	$131.9mil
Ave. Volume:	445,000
Instit. Ownership:	37%
BV / Share:	$0.96
Debt / Tot. Cap.:	0%
Est. LT EPS Growth:	10%-15%

Company Description

Entrust is a leading supplier of Public Key Infrastructure (PKI), device authentication applications, and related validation systems, software and services. Global enterprises and governments use Entrust products to secure logical and physical access control negotiations and transactions, ID cards, MRTDs, networks, PCs, PDA's, the Internet, doors, gates and borders.

KEY POINTS:

- **New products growing quickly.** *IdentityGuard, Boundary Messaging* and *Shared Network Folder* products represent new security applications, underpinning growth. 2H'07 revenue from financial institutions decreased 37% y/y with the sub-prime debacle. However, we expect bookings and revenue growth to resume going forward. Emerging growth products were 24% of Q4'07 product revenue. *IdentityGuard* transactions increased to 194 in FY'07, growing 98% year over year. *IdentityGuard* revenue surpassed $11.0 million in FY'07 and now represents over 9 million users worldwide.
- **Demand for PKI rebounding.** Entrust's core business is in Public Key Infrastructure and related system applications. Governmental regulatory and legislative mandates, like FIPS201, ICAO 9303 and national ID programs will drive new adoption waves for PKI, certificate and validation services. Entrust's PKI products/services accounted for 70% of FY'07 revenue, growing 11% year over year. Core PKI product revenue grew 40% in FY'07, while SSL certificate product revenue grew 32%. We believe the street under appreciates PKI's viability as a security application. Near term catalysts include large scale government credentialing programs, new security standards for online transactions and physical access control.
- **Fast growing subscription revs now exceed 51% of total revenue.** The Company is transitioning from a traditional perpetual license model to a more predictable subscription model. New "Security Software as a Service" models generate highly predictable and recurring cash flows, lower the Company's risk profile and could deserve substantially higher valuation premiums along side other SaaS/ASP models.
- **Improving fundamentals and visibility make ENTU cheap.** Entrust completed 472 transactions (+46%) and added 133 new customers (+64%) in FY'07. However, in our opinion, FY'07 financial results suffered, as large financial institutions deferred security/IT spending after sub-prime related issues. We currently estimate FY'08 revenue and pro-forma EPS of $108.9 million and $0.11, respectively. Further, we estimate FY'09 revenue and pro-forma EPS of $121.3mm and $0.17, respectively. Historically, PKI and device authentication related companies have traded at 3.7x sales. Today, Tier-2 comparables trade at roughly 70x FY'08 EPS estimates and 2.6x FY'08 revenue estimates. Further, Tier-2 comps trade at roughly 55x FY'09 EPS estimates and 2.2x FY'09 revenue estimates. Given Entrust's and its Industry's limited profit history, we have established a price target of $4.50 for ENTU, assuming ENTU trades at parity with the groups FY'09 Price/sales multiple.

SUMMARY:

We are initiating coverage of Entrust, Inc. with a STRONG BUY rating. We believe recent weakness in Entrust's reported financials and resultant stock weakness will abate as demand for Entrust core and emerging products accelerates throughout FY'08 and FY'09. We expect shares of ENTU can appreciate materially as a result. In our view, demand for Public Key Infrastructure (PKI) will boom as new privilege entitlement, credentialing and access control standards will force a new and large adoption cycle for PKI, Secure Socket Layer certificates, validation authorities and other identity and device authentication systems. Large systems integrators and vendors have been acquisitive and we consider Entrust to be a likely acquisition target. After a rocky FY'07, the Company recently turned profitable and anticipates continued growth in revenue, cash flow and profit. Our research shows that, at parity with its peer group's valuation trends, ENTU would trade at $4.50 per share. This represents over a 200% potential return and justifies a STRONG BUY rating.

Company Description

Entrust is a global provider of software, systems and services that are used to secure identities and information in physical and logical access control negotiations and transactions. Entrusts products authenticate and validate the identities of individuals and devices by ensuring the integrity of data in storage or in transport. With over 1,650 enterprise customers in over 60 countries and with over 100 patents or patent applications, Entrust's products are highly regarded by industry analysts, governments and enterprises worldwide.

Entrust Public Key Infrastructure and Entrust Authority

Entrusts certificate authority (CA) server is the backbone of many of its digital identity offerings. Entrusts Authority Manager was the first CA to receive Federal Information Processing Standard 140-1 certification and the Common Criteria certification. Entrust sells its Authority directly or through robust enterprise channels. The Company has traditionally sold PKI through classic client/server/seat architectures, charging per licensed user. Recently, however, Entrust has offered PKI and certificate validation as a hosted service, particularly for large government applications like new E-passports, national IDs and other machine readable travel documents (MRTD), charging a recurring subscription fee. Entrust PKI products and services represent the vast majority of Entrusts revenue to date.

Entrust IdentityGuard, Entelligence and Boundary Messaging Suites

In October 2005, The Federal Financial Institutions Examination Council (FFIEC) recommended that financial institutions implement enhanced authentication methods for online banking systems that go beyond simple "user-ID/password" systems. Entrusts product suites offer a new and comprehensive authentication platform that allows stakeholders to apply a measured approach when the strongest authentication may not be required. IdentityGuard primarily offers a matrix card, plus other potential security measures, to help ensure true user identity. The Entrust Entelligence messaging Server appliance secures data in transit. This product portfolio includes desktop and server based security capabilities for email, file and folder protection and remote access.

Recent Results:

Entrust recently reported Q4'07 revenue, GAAP-EPS and pro-forma EPS of $26.7mm, $0.02 and $0.04, respectively. Q4'07 results generally exceeded expectations after the Company reported a series of disappointing financial results. Importantly, some $2.5mm of revenue slipped from Q4'07 and foreign currency translation negatively affected Q4'07 revenue by roughly $5.0mm. For FY'07, ENTU reported revenue, GAAP-EPS and pro-forma EPS of $99.7mm, ($0.10) and $0.01, respectively. The Company generated roughly $750k in operating cash flow (CFO) in FY'07 and closed the year with about $20.5mm in cash and deferred revenue of over $27.5mm.

Outlook and Valuation:

Entrust management targets 1H'08 revenue, GAAP-EPS and pro-forma EPS of $50.0-$53.0mm, ($0.01) and $0.03, respectively. Further, management forecasts Q1'08 pro-forma expenses of roughly $25.0 million. For the year, the Company forecasts revenue, GAAP-EPS and pro-forma EPS of $106.0-$110.0mm, $0.02 and $0.10, respectively. Management also suggests FY'08 CFO, excluding accrued restructuring charges, will reach $10.0mm. Tier-2 comparables currently trade at 2.2x FY'09 revenue. Trading at parity with the group, shares of ENTU would trade at approximately $4.50.

Conclusion:

We are initiating coverage of Entrust, Inc. with a STRONG BUY rating. Our view is that new privilege entitlement, credentialing and access control standards will force a new and large adoption cycle for public key infrastructure and related applications. Our research shows that ENTU would be $4.50 at parity with its peer group's current valuation and could be an acquisition candidate. Consequently, we believe Entrust offers a compelling investment opportunity and recommend aggressively purchasing shares of ENTU at current levels.

Key Customers and partners

As of December 2007, the Company has licensed software to over 1,650 customers in 60 countries. Entrusts customers are often governments and Global 1500 enterprises in the financial, healthcare, telecomm and industrial industries. In Q4'07, Entrust achieved the following successes:

-- Entrust was chosen to provide PKI and secure e-mail to the **Saudi Arabian government** for their national ID project and to provide security for their e-government rollout, which would protect some 27 million citizens.

-- **SC Magazine** named Entrust as a finalist for the Excellence Award Best Security Company category. IT-security vendors nominated their solutions for consideration in SC Magazine's Awards program, and entries were judged by a panel of 18 leading chief security officers from major corporations and large public-sector organizations.

-- Entrust launched a custom selection of solutions to help enhance security for **Microsoft Exchange Server 2007** environments. Entrust offered three components of its layered security approach to enhance security for this powerful communication tool -- Entrust Unified Communications Certificates (UCC), Entrust Entelligence Messaging Server and the Entrust IdentityGuard versatile authentication platform.

-- Entrust launched the latest version of the versatile authentication platform: Entrust IdentityGuard 9.0. The release added new authentication options like IP-geolocation and included integration with the Entrust open fraud intelligence network (OFIN).

-- The Entrust IdentityGuard versatile authentication platform was chosen to secure and authenticate the identities of **Open Solutions** clients. Open Solutions leveraged Entrust IdentityGuard -- specifically the solution's grid card authenticator -- to its customer base, which primarily consists of financial institutions with assets less than $20 billion.

-- **Banco Central del Ecuador** deployed components of the Entrust layered security model, which included Entrust TruePass for zero-footprint public key infrastructure (PKI) capabilities; Entrust GetAccess for Web single sign-on (SSO); and the Entrust IdentityGuard versatile authentication platform for a range of strong authentication capabilities.

-- **NASA** partnered with Entrust to secure their 'One NASA' initiative. In order to maximize its IT security resources, NASA minimized overhead by using the **Department of Treasury's Shared Service Provider** (SSP) PKI service for digital certificates.

-- Entrust public key infrastructure (PKI)-enabled digital signatures continued to secure **U.S. ePassports. The U.S. State Department** reached the 20 million milestone in December for total ePassport deployment. The digital signatures on ePassports illustrated how PKI technology is being used in a number of new applications, reinforcing PKI as the gold standard for digital security.

-- **ICICI Bank**, India's largest private sector bank with assets of more than $92 billion, selected Entrust to provide standard SSL certificates -- a key component of a layered security approach -- to protect their valuable customers when conducting transactions on the institution's Web site. As part of the agreement, ICICI Bank standardized on Entrust SSL certificates for a five-year contract period.

Other customers include:

California Highway Patrol	Commonwealth of Kentucky	U.S. Dept. of Treasury
U.S. Dept. of Energy	Fed. Bureau of Investigation	Govt. of Canada
Canadian Public Works	Pacific Northwest Nat. Labs	RCMP
Quebec	Sacramento Utilities	SWBSADIS
Florida Comm. Affairs	State of Illinois	TeraNet
UK National Health Serv.	UK Office of e-Envoy	U.S. Dept. of Labor
U.S. Federal Bridge CA	U.S. Patent & Trademark	U.S. State Dept.
Canadian Veteran Affairs	Bank of Bermuda	CAIXA-Brazil
Chase Manhattan Bank	China Financial Cert. Auth.	Credit Suisse
Egg	Mackenzie Financial	Peoples Bank of China
U.S. Bank	Baptist Health	BC/BS Michigan
IDX Systems	Trac Medical	Compaq Corp.
Enel Group	Eurofighter GmbH	Ing Direct
KPN	Novartis	Perot Systems
Schlumberger	SILA Communications	TeleDanmark Comm.
Thomson Multimedia	Vodafone Corp.	

Key partners include:

Accenture	ActiveIdentity	Adobe Systems	Aladin Knowledge Systems	
CheckPoint	Cisco Systems	Cognos	CoreStreet	
Deloitte & To.	EDS	Gemalto	HP	IBM
Infineon Tech.	Juniper Netwrks	LabCal Tech.	Lockheed Martin	Lucent
Microsoft	nCipher Corp.	NEC Corp.	Nortel	Northrop Grumman
Novell	Oberthur Card	Oracle	Red Hat, Inc.	
RIMM	SafeNet	SETECS	Siemens	SSP-Litronic
Sun Microsyst.	Tibco	Tumbleweed Comm.		Unisys
Vignette	Webmethods	Waveset	WinMagic	Zebsign AS

Favorable Catalysts Ahead

- **Increased traction in emerging growth products.** We expect natural demand for emerging products like IdentityGuard and Boundary Messaging to drive substantial product growth rates.
- **FIPS201 Contract Awards.** We believe Entrust PKI, certificates and CA products currently represents the majority of non-DOD Federal PKI infrastructure, through its work at the U.S. Dept of Treasury and the Federal Bridge Authority. Given the "stickiness" of PKI solutions, we expect Entrust to capture the majority of FIPS201 related PKI business from civilian Federal agencies.
- **E-Passport Rollout.** Roughly 50 countries around the globe are in the early stages of deploying new ICAO 9303 compliant "E-passports". Roughly 180 countries around the globe must eventually deploy "E-passports". Entrust has been awarded a contract to supply the U.S. State Department its certificate applications for U.S. E-passport services. We expect other countries to follow suit.
- **Continued Industry Consolidation.** Several potentially comparable companies have been acquired or are in the process of being acquired. The most notable might be EMC Corp's acquisition of RSA Security (RSAS). RSA is a direct competitor to Entrust. We note that EMC offered to pay 6.1 times sales for RSA, or roughly $28 per share, while ENTU trades at roughly 1.1 times sales. We expect further consolidation in the space. Given Entrust's robust intellectual property and dominant position in the PKI space, we view Entrust as a potential acquisition candidate.

Why are Public Key Infrastructure (PKI) and Entrust Important in overall security?

Because we can no longer trust that you are who you say you are.

The 9/11 tragedy exemplified risks with insufficient credentialing and access control, while identity theft and fraud are pervasive, costing society billions annually. The FTC estimated identity theft victims in the year ending in May 2003 totaled 9.91 million individuals, with losses totaling $52.6 billion ($47.6 billion to businesses and $5 billion to individual victims). E-communication and e-commerce have only amplified our credentialing vulnerabilities. Our applications to establish or maintain trust are broken.

International and domestic governments have re-examined global credentialing, privileging, and access control systems. Significant research and development has produced new technology standards, application profiles and best practices, which are visible today. The modern secure credentialing platform, also known as **Personal Identity Verification (PIV)**, associates a privilege authorization with a person, links the person to a device, and then authenticates both the device and the person during the access control negotiation.

What is Personal Identity Verification?

At the most rudimentary level, a modern PIV system performs two basic tasks. It approves good people and rejects bad people. From another view, the application **identifies** safe people and **verifies** their identity as they approach. Anyone else is presumed to be bad and is denied. It answers the questions **"Who are you?" "Are you someone we will grant access to?"** and then **"Are you who you say you are?"** However, it's not all that simple because we must establish access control privileges for **physical access control (PACS)** (doors, gates, borders, etc.) and also **logical access control (LACS)** (computers, networks, internet, etc.). Historically, we separated the two authentication functions, attempting to automate them using completely independent technologies.

Logical Access Control Systems (LACS)

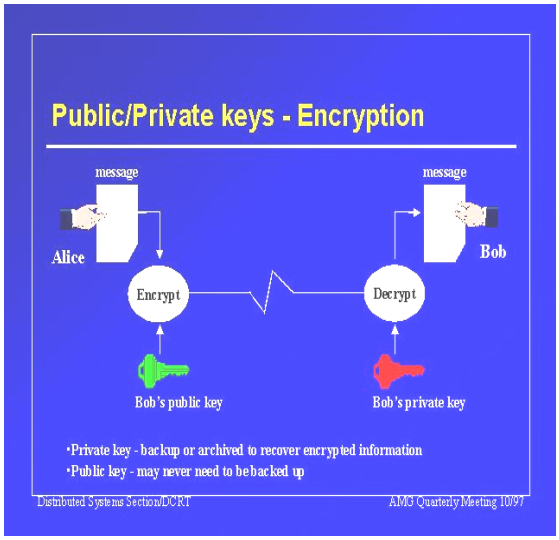
We typically attempt to control logical domains by **authenticating a device.** After all, people don't physically enter a computer network. People loosely interface with a logical domain through a personal computer or other portal device like a cell phone, PDA, etc. These systems are **Logical Access Control Systems** and answer the question **"Is this device or object allowed to interface with our device?"** One widely recognized device authentication application is **public key infrastructure (PKI).** It's presumed that anyone using an authenticated device is acceptable. However, controlling logical domains by authenticating and verifying the approaching device relies on false logic because, in reality, **we don't care much about the device; we care more about the person using the device**. To the point, an unauthorized person could use an authorized device to gain unauthorized access. Of course, "hacking" is a huge problem and we believe the obvious gravity of the hacking problem today is testament enough to the inadequacy of exclusive reliance on device authentication for logical access control, or any access control. Ironically, the modern solution strives to incorporate both PACS and LACS functionality into the same platform, **authenticating the device and the person for every access control transaction.** Modern access control thinking proposes to accomplish these tasks by combining distinct, and previously exclusive technologies into a symbiotic system.

Device Authentication and Public Key Infrastructure (PKI)

The modern secure credentialing and identification system is unique in that it forces the convergence of historically disassociated physical and logical access control applications. The new privileged authorization and access control platform authenticates devices and it authenticates people. **For our purposes, a device is anything that functions as a gateway or key representing access authorization to a logical domain or a physical domain.** For example, a PC acts as a gateway between a human being and a logical domain or cyber space. Many different technologies serve as logical domain portals. PCs, cell phones, PDAs, laptops and game consoles all act as our gateways to the electronic dimension. Many devices serve as a key to unlock the domain portal device. Tokens, ID cards, storage devices and smart cards are good examples of logical domain portal keys. Conversely, ID cards, smart cards, proximity cards, PINS and traditional keys have historically represented physical access authorizations for doorways, gates, etc. Interestingly, both applications have utilized many of the same types of portal or keys, but have traditionally been completely separate. We believe those functions will converge into one basic key. **We believe that the key (device) will ultimately be a smart card.**

Logical Domain

We keep and do many important things in the **logical domain**. We store important information and property, we communicate with one another, we transact business and share property in the logical domain. These activities and things are valuable and, as such, are targeted by thieves and vandals. The logical domain is structured rather simply. There are places where things are stored and mediums that carry things from one place to another. Thieves steal from the places things are stored, or by intercepting things as they travel from one place to another. The most common form of securing the logical domain is a concept called **Public Key Infrastructure (PKI).** PKI uses firewalls, encryption (cryptography), and "keys" to perform basic security tasks. **Firewalls keep everyone out. Encryption scrambles information into illegible secret code. Keys represent access authorization through the firewall or to descramble the communication.** Access through the firewall or to the data is denied without a valid "Public Key." The public key is often referred to as a **Certificate of Authority** and is purposefully attached to the devices representing known and trusted people. **The Certificate Authority (CA) performs the administration of PKI certificates.** The CA associates valid certificates (keys) with authorized devices, which are associated with authorized users. The CA also manages the list of revoked, or otherwise invalid certificates, called the **Certificate**



Revocation List (CRL). Inbound devices, or data objects like an email, verified by a valid certificate (public key), are accepted for interface. The CA rejects inbound portal devices or objects not verified by a validated key. It's presumed that anyone using a keyed portal device is trusted and privileged. This fact, in our opinion, is the first of two major problems with PKI. First, PKI relies on false logic because, in reality, we don't care much about the device; we care about the person using the device. To the point, an unauthorized person could use an authorized device to gain unauthorized access. Second, PKI can become increasingly expensive over time as the CRL often grows, especially in large and dynamic organizations, requiring larger and more costly storage applications. As the CRL grows, increasingly large lists of revoked certificates must be centrally stored or downloaded to access control sites for comparison against incoming device keys. This storage/cost dynamic has propelled another offshoot PKI application called **Online Certificate Status Protocol** (OCSP). OCSP acts as an outsourced CRL. An access request prompts a certificate validation query to the OCSP server, which responds with "current," "expired" or "unknown," facilitating an acceptance or denial.

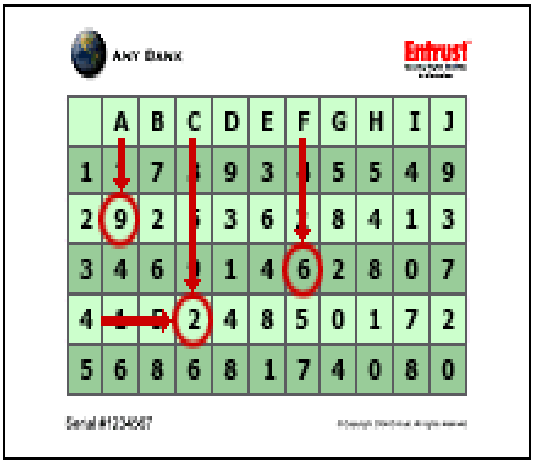
Secure Socket Layer (SSL) certification and why it isn't all you need

There are basically four "elements" within a communication relationship: the sender, the sent object, the transmission medium (the pipe) and the receiver. To properly secure a communication, all four elements should be secured. Practically speaking, securing transmission mediums (pipes) and objects is easier (and much cheaper) than securing individual identities. Ease of deployment, expense aversion and basic ignorance has historically motivated stakeholders to pursue the path of least resistance, largely avoiding PKI and biometrics. Conversely, major stakeholders have assumed that by securing the ends of the "pipe" and by assuming the user is safe, the entire communication structure is automatically and completely safe. Secure Socket Layer (SSL) certification is the primary method of securing transmission mediums (the pipe). SSL presumes to secure the pipe by certifying web servers and then authenticating each web server by validating the assigned certificates represented on either end of the communication channel. Verisign Corp. dominates this business, controlling over 50% of this market. The problem is that SSL does little to ensure that people at opposing ends of the pipe are actually safe to communicate with. PKI, in combination with biometrics, completes the "chain of trust". By attaching keys to the personal devices like PCs and cell phones, we can validate devices that connect to the web server. By authenticating the user with a biometric, we attach the user to the authorized device. Relying exclusively on SSL without PKI and biometrics is like assuming a driver's license is valid because nobody has broken into the Department of Motor Vehicles recently. It's not safe. We believe the technology now exists and stakeholders are sufficiently motivated to complete the "chain of trust", deploying PKI and biometrically enabled smart cards for truly strong user and communication authentication.

Closing the vulnerability

In an attempt to close the false logic vulnerability, many device authentication vendors "personalize" the device by scrambling the public key and requiring a "Private Key," plus a PIN, to decode the "Public Key." If you don't have the PIN or password, you can't decrypt the public key. However, people are often lazy, utilizing PINs or passwords that are easy to guess or simply listing them in public view: taped to their PC, for example. Attempting to close this vulnerability, device authentication vendors offered new, even more personalized keys called **tokens**, sometimes in combination with random number (PIN/key) generator applets. Tokens are simply yet another device, a small personal electronic device containing data, extending the device authentication false logic by an additional degree of separation. Tokens serve as another key and are often designed to attach to a key ring, literally. Tokens interface with the portal devices, prompting for the private key. Thus, the token must be present, in addition to the private key, plus PIN potentially, to unlock the public key. Some argue that

tokens are an even more expensive way to extend and personalize the public key access privilege. Others argue that random key generators eliminate the important personalization (something only you know). Recent attempts to overcome this price obstacle include simplifying the token by replacing it with a wallet-sized card that contains a matrix of numbers or images. Upon access authorization request, the cardholder enters a PIN and is prompted to enter randomly selected numbers/images located in grid locations on the card. Without the card, the user would lack required data and be denied access. While this "bingo card" may reduce cost, it does nothing to reduce the false logic vulnerability beyond existing capabilities. We imagine users writing their PIN numbers, most likely their birth dates, on the bingo card before it's stolen or lost. Maybe they will tape the bingo card on the PC, right next to their PIN. "Access Approved!" Consequently, in our opinion, it simply cuts cost, which is why, in our opinion, the financial community appears to endorse the concept. An interesting idea, but it doesn't really solve the security problem. We view it as a temporary patch or bridge. In our opinion, the token and the bingo card will lose their appeal as smart cards and biometrics roll out. The smart card (device) will replace the token and could reduce cost as numerous applications converge into the one device. It will be encrypted and authenticated with keys. The biometric and PIN will authenticate the user and require the cardholder's presence during access control negotiation. This will take time to roll out, of course, providing a solid near-term market for bingo cards.



The PKI Marketplace

How big is the PKI market? In our opinion, the PKI market is conceptually so big that it's almost unbelievable. However, current-pricing models could help gain perspective on this application marketplace potential and its pitfalls. PKI, as it's typically designed, utilizes the classic server/client/seat architecture. Ball-park pricing a rudimentary system, we estimate a normalized server prices around $25,000, providing basic CA and CRL functionality, plus around $10-$14 per certificate, or "seat." Depending on the size or structure of the program, OCSP may be required. Now, simply count seats, right? Well, not exactly.

This price dynamic fails to incorporate storage and ongoing hosting costs as the CRL invariably changes and grows. Consider a large corporation with 100,000 employees scattered across several geographies. Each employee receives a certificate. Naturally, there is some annual employee turnover. Each employment termination generates a revocation on the CRL. Employees may enjoy entitlements between departments or managerial levels, requiring several certificates.

The Numbers Tell the Story

Global Metrics	1995 early Adoption	2000 Max Hype	2005 Serious Use	2010 Everyday Life	% Change
Internet Users	16m	368m	888m	1.5b*	9,275
DNS Queries	20m	2b	14b	45b	160,614
E-mails Sent	8.4b	600b	1.5t	2.7t*	32,043
E-commerce	$3b	$100b	$142b	$307b	10,133
Mobile Phone Users	90m	450m	1.6b	1.7b	1,789
SMS messages		38b	960b	1.3t	3,321
Mobile Commerce		$127m	$13b	$58b	45,884
* Projections for 2007					

Source: 2005: Internet World Stats, Computer Industry Almanac, UVA, MRG, SIMS, eMarketer and VeriSign

What about visitors? Some keys may be temporary, but certificate records may be required for some time. Some employees may move within departments, or geographies, etc. Geography alone could require several independent CAs and CRLs. Each new certificate consumes capacity on the CA. Each certificate revocation adds to the CRL. Every time an access request is submitted, the system must compare the inbound certificate against the CA and the CRL. Consequently, the CRL must be frequently refreshed, potentially every few days or even hours. Moreover, that CRL may need to be distributed to various locations. We could easily demonstrate how this 100,000 employee firm could require hundreds of thousand of certificates over time, at $10-$14 per certificate.

Now consider the market potential relative to the Internet. According to the VeriSign chart above, there were 888 million Internet users and 1.6 billion mobile phone users in 2005. Most, if not all, of these consumers are "keyed". Moreover, the growth rates of those populations are is significant. According to this chart, there were 1.5 trillion emails sent and 960 million SMS messages sent. In a truly secure world, each "user" would be assigned at least one key for every service they opt into, plus additional keys as more devices are introduced into the identity profile. Each email, each DNS query, and each SMS message, from any or all PC's, laptops, PDAs and cell phones should be "keyed." Suffice to say, we are talking about a lot of potential certificates.

For our secure credentialing purposes, we note that ICAO estimates there are roughly 550 million passports in circulation today and that number is expected to grow quickly over the next ten years. At $10 per certificate, the passport market could approach $5.5 billion over a 10-year period. According to the U.S. Department of Transportation, there were approximately 199 million licensed drivers in the United States in 2004. Assuming drivers licenses become "smart", each would likely require at least one certificate, depending on how

many different services the credential is expected to interface with. At $10 per certificate, the U.S. driver's license market, alone, could approach $2 billion or more, spanning several years. We note that many countries are enacting national ID card programs. Most of these are smart cards, storing important personal data that would require PKI. In truth, virtually any credentialing program is a target market for device authentication applications like PKI. Those certificates must all be managed and accounted for somewhere. Consequently, we are comfortable suggesting the market place is potentially very large, growing and likely recurring.

Biometric-like Behavior Profiling takes personalization closer to the person

Recent fads in "anti-fraud" and Personal Identity Verification include rekindling behavior pattern recognition applications. These applications take note of use patterns like keystroke dynamics, destination, surfing and other behavior patterns. These patterns and habits can be represented in a profile that is associated with the individual or identity. Any material deviation from the pattern profile could trigger an alert, or even a complete capability disruption, at least until the users identity can be confirmed. For example, if your profile does not include frequenting pornographic websites, the system may alert administrative services that something may be wrong if/when the device attempts to engage a pornographic site. The assumption is that since the device is doing something it normally wouldn't, behaving abnormally outside the profile, the user may not be the authorized user. The administrative service could automatically disable various capabilities, including e-commerce capabilities, pending further identity verification tests. To this end, these behavioral profiling algorithms and applications emulate a biometric verification, attempting to attach the approved user to the specific transaction. The systems attempt to ensure that the person at the keyboard, or other device, is actually the authorized user. However, these systems really do little more than automate call center monitoring of access control and/or financial transactions, a common practice today in the credit industry.

There are a few problems with these profiling applications. First, their accuracy has not been independently validated that we are aware. As such, Government, especially the Federal government, and administrators requiring high security won't likely rely on these applications. Second, these algorithms are only as discerning as the administrator prefers. Their sensitivity to behavioral anomalies and profile rule violations can usually be adjusted higher or lower, allowing more frequent or more amplified deviations from the profile (the mean). Thus, transactionally biased institutions, those in favor of more frequent and easier transactions, or service providers concerned about potential customer inconvenience may be motivated to desensitize the system, allowing less scrupulous security screening and more frequent or amplified deviations from a properly vetted profile. Given that financial institutions currently pass fraud related costs to consumers via higher interest rates and charges, and given that consumers don't seem to mind, we expect financial institutions to demand and pay for only the minimum security threshold required.

Regulation and legislation requires new security and identity verification solutions.

Gramm-Leach-Bliley Act: This act requires stringent adherence to the Financial Privacy Rule and the Safeguards Rule, which require institutions to develop more advanced consumer data privacy policies, procedures and infrastructures. It also requires institutions to disclose those policies, procedures and infrastructures to customers at least annually.

California SB1386: This California law requires institutions to guard against identity theft and to publicly disclose any breach or theft of consumer identity related data.

FFIEC: On October 12, 2005 the Federal Financial Institutions Examination Council (FFIEC) issued the updated guidance, "Authentication in an Internet Banking Environment." which requires that banking institutions guard against fraud and identity theft by implementing, at a minimum, a two factor authentication technique to verify the identity of on-line customers.

ICAO 9303: In March 2003, the International Civil Aviation Organization (ICAO) issued new technology specifications for Machine Readable Travel Documents, including passports, visas, and drivers licenses. The new specifications (ICAO 9303) require these credentials to utilize a contactless integrated circuit chip (IC) to contain data about the credential holder, including biometric, demographic and biographic data. This data is to be secured by cryptography in a public key infrastructure.

HSPD-12: Homeland Security Presidential Directive #12 requires that all Federal employees and contractors carry a new standardized identification credential. The credential must comply with Federal Information Processing Standard #201 (FIPS201), including smart card technology, biometrics, and certificate validation (PKI).

HIPPA: The Healthcare Information Privacy and Portability Act requires that healthcare related industries ensure the privacy of all patient data. Related information systems must utilize multi-factor authentication strategies.

Therefore, Matrix Cards and Behavior Profiling can be successful over the short run
Conceptually, this type of application makes sense. In reality, however, it's merely a baby step toward full-blown biometric identity verification. We believe short term demand for matrix card platforms and behavior profiling algorithms will be relatively significant because they presume to solve real security and identity verification problems with a relatively small capital outlay. In our opinion, these systems should not be heavily relied upon for the reasons we have already discussed. Therefore, we believe these technologies are short run applications. As reported, laws and regulations require the adoption of more sophisticated, but not the most sophisticated, security and identity verification techniques. In particular, California SB1386, Gramm-Leach-Bliley, Basel-2 and the FFIEC guidance increases pressure on organizations, specifically consumer data and financial institutions, to improve security. In our opinion, subject organizations are likely to perform to minimum standards and will be inclined to minimize security related expenditures and hassle. Conversely, ICAO 9303, FIPS201 and other application profiles demand substantially higher authentication methods including biometric and PKI emboldened smart cards. Therefore, in our opinion, matrix cards and behavior profiling could satisfy cost requirements, at least until truly strong, long run solutions like biometric and PKI enabled smart card solutions can be implemented. In our opinion, demand for PKI and biometrics will grow significantly as the two technologies are paired together.

Investment Conclusion

We are initiating coverage of Entrust, Inc. with a STRONG BUY rating. While we appreciate near term commercial opportunities for new product offerings, we believe the street under appreciates market opportunities for traditional PKI products and services. Our view is that new privilege entitlement, credentialing and access control standards will force a new and large adoption cycle for public key infrastructure. Our research shows that ENTU would be $4.50 at parity with its peer group's valuation based on 2.2x FY'09 revenue. Furthermore, we believe ENTU could be an acquisition candidate. Consequently, we believe Entrust offers a compelling investment opportunity and recommend purchasing shares of ENTU at current levels.

Income Statement	Full-Year	Full-Year	Full-Year	Full-Year	Q1	Q2	Q3	Q4	Full-Year	Q1E	Q2E	Q3E	Q4E	Full-Year	Full-Year
Millions	2003	2004	2005	2006	Mar-07	Jun-07	Sep-07	Dec-07	2007	Mar-08	Jun-08	Sep-08	Dec-08	2008E	2009E
Total Revenue	87.9	91.0	98.1	95.2	24.6	24.5	23.9	26.7	99.7	26.3	26.7	26.6	29.3	108.9	121.3
Cost of Sales	35.7	33.6	36.5	37.8	9.5	10.1	9.3	10.2	39.1	10.1	10.2	9.9	10.7	40.8	44.9
Gross Profit	52.2	57.3	61.7	57.4	15.1	14.3	14.7	16.4	60.6	16.3	16.5	16.7	18.5	68.0	76.4
Gross Margin	*59.3%*	*63.0%*	*62.9%*	*60.3%*	*61.4%*	*58.6%*	*61.3%*	*61.7%*	*60.8%*	*61.7%*	*61.8%*	*62.9%*	*63.3%*	*62.5%*	*63.0%*
Sales & Marketing	$ 35.0	$ 26.3	$ 28.5	$ 33.3	$ 8.6	$ 8.3	$ 7.7	$ 7.7	$ 32.2	$ 8.1	$ 8.1	$ 7.8	$ 8.5	$ 32.5	$ 35.2
% of Revenue	*39.8%*	*28.9%*	*29.1%*	*35.0%*	*34.9%*	*33.7%*	*32.1%*	*28.9%*	*32.3%*	*30.8%*	*30.3%*	*29.4%*	*29.0%*	*29.9%*	*29.0%*
Research/Development	22.6	17.3	16.4	19.6	5.2	5.1	4.8	4.6	19.6	4.8	4.7	4.7	5.0	19.2	20.8
% of Revenue	*25.7%*	*19.0%*	*16.8%*	*20.6%*	*21.0%*	*20.9%*	*19.9%*	*17.1%*	*19.6%*	*18.2%*	*17.6%*	*17.7%*	*17.1%*	*17.6%*	*17.1%*
General & Administrative	13.1	12.6	11.5	13.7	2.8	2.8	2.4	2.9	10.9	3.0	2.9	2.8	3.1	11.8	12.8
% of Revenue	*15.0%*	*13.8%*	*11.8%*	*14.4%*	*11.5%*	*11.2%*	*10.1%*	*10.8%*	*10.9%*	*11.4%*	*10.9%*	*10.5%*	*10.6%*	*10.8%*	*10.5%*
Intangibles, Restrct, FASB123	17.5	-	-	5.6	1.3	1.4	1.3	0.9	4.8	1.2	1.2	0.9	0.9	4.2	3.6
Total Operating Expense	88.2	56.2	56.5	72.3	17.8	17.5	16.2	16.0	67.5	17.1	16.9	16.2	17.5	67.7	72.4
% of Revenue	*100.3%*	*61.7%*	*57.6%*	*75.9%*	*72.5%*	*71.5%*	*67.5%*	*60.1%*	*67.7%*	*65.1%*	*63.3%*	*61.0%*	*59.6%*	*62.2%*	*59.7%*
Operating Income	(36.0)	1.2	5.2	(13.8)	(2.7)	(3.2)	(1.5)	0.4	(7.0)	(0.9)	(0.4)	0.5	1.1	0.3	4.0
Operating Margin	*-41.0%*	*1.3%*	*5.3%*	*-14.5%*	*-11.1%*	*-12.9%*	*-6.2%*	*1.6%*	*-7.0%*	*-3.4%*	*-1.5%*	*1.9%*	*3.7%*	*0.3%*	*3.3%*
Net Interest $ Other Expenses	0.6	0.6	1.7	(1.5)	0.4	(0.0)	0.1	0.6	1.2	0.1	0.1	0.2	0.2	0.6	1.4
% of Revenue	*0.7%*	*0.7%*	*1.8%*	*-1.6%*	*1.7%*	*0.0%*	*0.4%*	*2.3%*	*1.2%*	*0.3%*	*0.5%*	*0.7%*	*0.7%*	*0.6%*	*1.1%*
Pretax Income	(35.4)	1.8	6.9	(15.3)	(2.3)	(3.2)	(1.4)	1.0	(5.8)	(0.8)	(0.3)	0.7	1.3	1.0	5.4
Pretax Margin	*-40.3%*	*1.9%*	*7.0%*	*-16.1%*	*-9.4%*	*-13.0%*	*-5.8%*	*3.9%*	*-5.8%*	*-3.0%*	*-1.0%*	*2.7%*	*4.4%*	*0.9%*	*4.4%*
Taxes	0.4	0.7	0.5	0.3	0.1	0.1	0.1	0.1	0.3	0.1	0.1	0.1	0.1	0.4	0.4
Tax Rate	*-1.2%*	*38.9%*	*7.7%*	*-2.2%*	*-2.3%*	*-2.3%*	*-7.5%*	*7.7%*	*-5.3%*	*-10.0%*	*-29.4%*	*14.1%*	*7.7%*	*37.3%*	*7.4%*
Net Income	(35.9)	1.1	6.4	(15.6)	(2.4)	(3.2)	(1.5)	1.0	(6.1)	(0.9)	(0.3)	0.6	1.2	0.6	5.0
EPS, excl. charges & FASB123	$ (0.56)	$ 0.02	$ 0.11	$ (0.10)	$ (0.01)	$ (0.02)	$ 0.00	$ 0.04	$ 0.01	$ 0.01	$ 0.02	$ 0.03	$ 0.04	$ 0.11	$ 0.17
Reported EPS	$ (0.56)	$ 0.02	$ 0.10	$ (0.26)	$ (0.04)	$ (0.05)	$ (0.02)	$ 0.02	$ (0.10)	$ (0.01)	$ (0.01)	$ 0.01	$ 0.02	$ 0.01	$ 0.08
Avg. Shares, Fully Diluted	63.6	64.0	62.8	59.7	60.4	60.8	61.0	61.1	60.8	61.1	61.2	61.3	61.4	61.3	61.7

Balance Sheet	Full-Year	Full-Year	Full-Year	Full-Year	Q1	Q2	Q3	Q4	Full-Year	Q1E	Q2E	Q3E	Q4E	Full-Year	Full-Year
ASSETS:	2003	2004	2005	2006	Mar-07	Jun-07	Sep-07	Dec-07	2007	Mar-08	Jun-08	Sep-08	Dec-08	2008E	2009E
Cash & Equivalents	37.9	36.3	59.9	22.5	20.8	24.2	21.5	20.5	20.5	22.9	22.5	26.2	25.0	25.0	40.5
Cash per Share	$ 0.60	$ 0.57	$ 0.96	$ 0.38	$ 0.38	$ 0.40	$ 0.35	$ 0.34	$ 0.34	$ 0.34	$ 0.37	$ 0.43	$ 0.41	$ 0.41	$ 0.66
ST Investments	54.4	61.0	22.5	-	-	-			-	-	-			-	-
Accounts Receivable	19.9	16.7	20.3	21.1	21.3	17.0	18.3	20.8	20.8	19.5	20.5	21.0	22.5	22.5	24.0
Prepaid / Other	2.9	3.4	4.8	2.9	3.1	3.4	3.8	4.1	4.1	3.8	4.0	4.1	3.9	3.9	2.1
Total Current Assets	115.0	117.4	107.6	46.5	45.1	44.6	43.6	45.3	45.3	46.2	47.0	51.3	51.4	51.4	66.6
LT Securities	-													-	-
LT Investments	12.4	2.0													
Goodwill	11.2	12.7	12.7	60.2	60.2	60.2	60.2	60.2	60.2	60.2	60.2	60.2	60.2	60.2	60.2
Property/Equip., Net	7.7	5.2	2.7	2.7	2.1	1.9	1.8	1.5	1.5	1.3	1.1	0.9	0.8	0.8	0.4
Purch. Product Right	-	2.9	2.1	13.8	13.3	12.7	12.2	11.5	11.5	10.6	9.6	8.9	8.3	8.3	5.8
Other Intangibles															
LT Equity Invest.	0.7	4.0	3.6	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Other Assets	1.8	1.7	1.8	4.3	4.3	4.1	3.8	3.5	3.5	3.3	3.9	4.0	3.6	3.6	2.7
Total Assets	148.8	145.9	130.45	127.82	125.1	123.7	121.7	122.2	122.15	121.6	121.8	125.4	124.3	124.34	135.81
LIABILITIES															
Accounts Payable	6.2	7.5	7.2	20.3	14.7	16.2	16.2	16.3	16.3	16.5	16.6	16.8	18.2	18.2	23.8
Accrued Liabs.	9.6	7.9	6.4	-					-					-	-
Accrued Restruct.	35.4	3.9	3.6	-	-	21.9	20.6	19.3	19.3	19.0	18.5	18.2	17.8	17.8	16.2
Current Liabilities	51.2	19.3	17.2	20.3	14.7	38.1	36.8	35.6	35.6	35.5	35.1	35.0	36.0	36.0	40.0
Total Long Term Debt															
Long Term Liab.	0.2	1.4	0.9	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
Deferred Revenue	16.6	23.0	20.9	23.6	28.3	28.5	28.2	27.9	27.9	28.6	31.0	33.2	34.0	34.0	38.0
Accrued Restructuring		26.2	22.4	24.5	23.3	-	-	-	-	-	-	-	-	-	-
Minority Interest		0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total Liabilities	68.1	69.9	61.3	68.6	66.5	66.8	65.2	63.7	63.7	64.3	66.3	68.4	70.2	70.2	78.3
SHAREHOLDERS' EQUITY	80.7	76.0	69.1	59.2	58.6	56.8	56.5	58.4	58.4	57.3	55.5	57.0	54.1	54.1	57.6
Total Liab. & Shareholders' Equity	148.8	145.9	130.4	127.8	125.1	123.7	121.7	122.2	122.2	121.6	121.8	125.4	124.3	124.3	135.8
Current Ratio	2.2	6.1	6.3	2.3	3.1	1.2	1.2	1.3	1.3	1.3	1.3	1.5	1.4	1.4	1.7
Working Capital	$ 63.80	$ 98.14	$ 90.39	$ 26.28	$ 30.39	$ 6.53	$ 6.83	$ 9.74	$ 9.74	$ 10.66	$ 11.93	$ 16.28	$ 15.40	$ 15.40	$ 26.54
Days Receivable	82.6	66.9	75.7	81.0	79.1	63.4	69.9	71.1	76.1	67.6	70.1	72.1	70.2	75.4	72.2
Days Payable	25.4	29.9	26.5	76.7	54.0	59.5	61.0	55.1	59.0	56.4	56.0	56.9	56.0	60.2	70.6
Book Value Per Share	$ 1.27	$ 1.19	$ 1.10	$ 0.99	$ 0.97	$ 0.94	$ 0.93	$ 0.96	$ 0.96	$ 0.94	$ 0.91	$ 0.93	$ 0.88	$ 0.88	$ 0.93
Cash Flow	(35.3)	1.5	7.2	(1.7)	(2.7)	2.9	(3.0)	(1.8)	(4.6)	2.4	2.0	3.3	2.5	10.2	15.5

Jay M. Meier
Feltl Co.
612-492-8847

2/6/2008

PKI and Device Authentication Valuations

Name	Ticker	LAST	ShrsOS(mill	Mkt Cap(mill)	2008E EPS	2008E Sales	2008E P/E	2008E P/S	2009E EPS	2009E Sales	2009E P/E	2009E P/S	12 mon ANNHI	12 mon ANNLO	% chg high/low
Computer Associates	CA	24.52	516	12,643	1.22	4,272	20.1	3.0	1.34	4,437	18.3	2.8	28.46	20.21	41%
Intl. Business Machin	IBM	105.20	1,378	144,966	7.18	104,573	14.7	1.4	8.27	109,522	12.7	1.3	121.96	88.21	38%
Microsoft Corp.	MSFT	29.07	9,307	270,554	2.10	60,198	13.8	4.5	2.37	66,439	12.3	4.1	37.5	26.60	41%
Verisign, Inc.	VRSN	33.83	221	7,476	1.06	935	31.9	8.0	1.65	1,106	20.5	6.8	41.96	23.78	76%
AVERAGE:				**108,909.76**			**20.1**	**4.2**			**15.9**	**3.8**			49%
Active Identity Sol.	ACTI	3.36	46	154	(0.19)	66.73	(17.7)	2.3	0.02	77.93	168.0	2.0	5.5	2.96	86%
Aladen Knowledge S	ALDN	21.60	15	318	1.34	125.07	16.1	2.5	1.55	141.95	13.9	2.2	26.94	16.60	62%
Tumbleweed Comm.	TMWD	1.73	51	88	0.01	60.54	173.0	1.5	0.09	70.74	19.2	1.2	3.66	1.18	210%
Vasco Systems	VDSI	17.16	37	638	0.89	164.99	19.3	3.9	1.23	207.5	14.0	3.1	44.25	14.50	205%
WidePoint ORC	WYY	1.29	53	68	na	na	na	na	na	na	na	na	2.26	0.02	11200%
AVERAGE:				**253.14**			**69.47**	**2.54**	**0.72**		**53.78**	**2.13**			2353%
Entrust, Inc.	**ENTU**	2.11	**61**	**129**	**0.11**	**108.9**	19.2	1.2	**0.17**	**121.3**	12.4	1.1	4.6	1.65	179%

Price Targets:	Tier One FY'08	Tier One FY'09	Tier Two: FY'08	Tier Two: FY'09
EPS:	$2.21	$2.71	$7.64	$9.14
Sales:	$7.50	$7.45	$4.53	$4.24

Analyst Certification

I, **Jay M. Meier**, certify that the views expressed in this research report accurately reflect my personal views about the subject company and its securities. I also certify that I have not been, am not, and will not be receiving direct or indirect compensation related to the specific recommendations expressed in this report.

Important Disclosures:

The analyst or any member of his/her household **does not** hold a long or short position, options, warrants, rights or futures of this security in their personal account(s).

Feltl and Company **does** make a market in the subject security at the date of publication of this report. As a market maker, Feltl and Company could act as principal or agent with respect to the purchase or sale of those securities.

As of the end of the month preceding the date of publication of this report, Feltl and Company **did not** beneficially own 1% or more of any class of common equity securities of the subject company.

There **is not** any actual material conflict of interest that either the analyst or Feltl and Company is aware of.

The analyst **has not** received any compensation for any investment banking business with this company in the past twelve months and **does not** expect to receive any in the next three months.

Feltl and Company **has not** been engaged for investment banking services with the subject company during the past twelve months and **does not** anticipate receiving compensation for such services in the next three months.

Feltl and Company **has not** served as a broker, either as agent or principal, buying back stock for the subject company's account as part of the company's authorized stock buy-back program in the last twelve months.

No director, officer or employee of Feltl and Company serves as a director, officer or advisory board member to the subject company.

Feltl and Company Rating System: Feltl and Company utilizes a four tier rating system for potential total returns over the next 12 months.

Strong Buy: The stock is expected to have total return potential of at least 30%. Catalysts exist to generate higher valuations, and positions should be initiated at current levels.
Buy: The stock is expected to have total return potential of at least 15%. Near term catalysts may not exist and the common stock needs further time to develop. Investors requiring time to build positions may consider current levels attractive.
Hold: The stock is expected to have total return potential of less than 15%. Fundamental events are not present to make it either a Buy or a Sell. The stock is an acceptable longer-term holding.
Sell: Expect a negative total return. Current positions may be used as a source of funds.

2/1/2008

Ratings Distribution for Feltl and Company

			------ Investment Banking ------	
Rating	Number of Stocks	Percent of Total	Number of Stocks	Percent of Rating category
SB/Buy	29	73%	4	14%
Hold	10	25%	0	0%
Sell	1	3%	0	0%
	40	100%	4	10%

Date	Nature of Report	Rating	Price Target
2/5/08	Initiation @ $2.16	SB	$4.50

Valuation and Price Target Methodology:

Historically, PKI and device authentication related companies have traded at 3.7x sales. Today, Tier-2 comparables trade at roughly 69.5x FY'08 EPS estimates and 2.6x FY'08 revenue estimates. Further, Tier-2 comps trade at roughly 55.1x FY'09 EPS estimates and 2.2x FY'09 revenue estimates. Given the Company's and groups limited profit history, we have established a price target of $4.50 for ENTU, assuming ENTU trades at parity with the groups FY'09 Price/sales multiple.

Risks to Achievement of Estimates and Price Target:

- Actual or anticipated fluctuations in operating results
- Announcements of technological innovations
- New products introduced by, or new contracts entered into by the Company or competitors
- Competition
- Developments with respect to intellectual property
- Changes in demand for security software applications in general
- Changes in financial estimates by securities analysts including Feltl & Co.
- General economic and market conditions
- Readers should recognize that the risks noted here do not represent a comprehensive list of all risk factors or potential issues, nor all factors that may preclude achievement of our forecast or price target. Additional risk factors exist and are outlined in the Company's SEC filings

Other Disclosures:

The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. This report has been

prepared solely for informative purposes and is not a solicitation or an offer to buy or sell any security. The securities described may not be qualified for purchase in all jurisdictions. Because of individual requirements, advice regarding securities mentioned in this report should not be construed as suitable for all accounts. This report does not take into account the investment objectives, financial situation and needs of any particular client of Feltl and Company. Some securities mentioned herein relate to small speculative companies that may not be suitable for some accounts. Feltl and Company suggests that prior to acting on any of the recommendations herein, the recipient should consider whether such a recommendation is appropriate given their investment objectives and current financial circumstances. Past performance does not guarantee future results. Additional information is available upon request.

EQUITY CAPITAL MARKETS
DIRECTORY

Feltl and Company
SECURITIES BROKERAGE AND INVESTMENT BANKING

RESEARCH DEPARTMENT

Clinton H. Morrison, CFA
Director of Equity Research
(612) 492-8878

Ernest W. Andberg, CFA
(612) 492-8836

Paul J. Axt
(612) 492-8837

Jay M. Meier
(612) 492-8847

Richard A. Ryan
(612) 492-8841

Mark E. Smith
(612) 492-8806

Jack M. Zipoy
(612) 492-8860

TRADING: (866) 777-9862

Joseph G. Fredericks
Manager, Equity Trading
(612) 492-8888

William W. Koop
(612) 492-8830

Thomas Walters
(612) 492-8829

Elliott Randolph
Institutional Sales Trading
(612) 492-8867

Cory Carlson
Institutional Sales Trading
(612) 492-8858

Luke J. Weimerskirch
Institutional Sales Trading
(612)492-8832

INSTITUTIONAL SALES: (866) 338-3522

Thomas Pierce
Senior Vice President – Institutional Sales
(612) 492-8817

Mark Hagen
(612) 492-8846

Ryan Quade
(612) 492-8807

Dugan Buffington
(612) 492-8862