



Secure eCommerce Transactions

The Volume, the Requirements,
the Path to a Solution

*An IDC White Paper
Sponsored by ValiCert, Co.*

John Daly, Roseann Day, and Charles Kolodgy

ABSTRACT

eBusiness continues to grow at exponential rates. Despite the drastic value deflation in pure-play Internet companies and overall economic trends, business conducted online continues to expand at impressive rates. IDC projects that ecommerce — the digital commitment of funds, often in exchange for goods or services over a network — will grow at impressive double-digit rates.

Despite setbacks, deflations, and security scares, businesses are moving steadily to streamline their procurement and payment processes by taking advantage of the Web. IDC projects worldwide business-to-business (B2B) ecommerce transaction values will grow from approximately \$450 billion in 2001 to more than \$4,000 billion in 2005. Additionally, the immense numbers of transactions that support ecommerce commitments (e.g., data gathering, bid development, information sharing, etc.) are increasing just as fast.

The promise for speedy, less expensive transactions does come with a price, however. B2B ecommerce transactions of either substantial value or a sensitive nature pose risks much higher than those normally encountered with business-to-consumer (B2C) activity. This white paper investigates this continuing ebusiness phenomenon and the IT security underlayment that must evolve to support ebusiness. The paper also looks at ValiCert's approach to enable these transactions and provide the infrastructure essential to conducting successful online business.

APPROACH

IDC developed this report using a combination of ecommerce market models, wide-scale quantitative customer surveys available to IDC, and direct primary research. To understand the most important security issues challenging ecommerce, we selected interviewees from six enterprises. We selected organizations that were working to extend ebusiness initiatives enough to handle sensitive, high-value transactions over the Web. This group of six interviewees included

www.idc.com

5 Speen Street • Framingham, MA 01701 USA • Phone 508.872.8200 • Fax 508.935.4015

organizations operating in the financial services, insurance, and healthcare industries. It also included leading executives from technology initiatives and enterprises that were preparing trust platforms for ecommerce initiatives. We conducted in-depth qualitative discussions with representatives from these organizations, exploring the particular issues and challenges they found most pressing. This paper reflects all of these research perspectives.

eCommerce Transactions: Definitions and Volumes

Setting the stage for ecommerce security involves defining ecommerce transactions. With definitions in place, we can then measure the volume and growth of ecommerce transactions.

First, IDC considers ecommerce a subset of ebusiness — the electronic automation or enhancement of the broadset activities around business processes. IDC defines ecommerce as the process of placing or accepting an order via the Internet, an online commitment for a transfer of funds in exchange for goods or services. eCommer- ce involves a number of steps:

- **Information gathering** — e.g., product or price information from a variety of sources
- **Engagement** — buyer and seller connect with each other
- **Negotiation** — discussion of product features, price, configura- tion, and so on
- **Commitment** — commitment to purchase a product or service — an order representing an obligation to transfer funds in exchange
- **Payment** — buyer offers payment information or currency to the seller
- **Fulfillment/delivery** — buyer receives the product or service

However, IDC includes only "the commitment and placement of an order over the Internet" as an Internet ecommerce transaction. Pay- ment on the Internet is not required for inclusion. IDC does call out a category of direct commerce, where the buyer provides payment information (e.g., credit card or electronic funds transfer) through the Internet at the time of commitment.

eCommerce will increase from approximately \$600 billion in 2001 to more than \$5,000 billion in 2005.

All of ecommerce will increase from approximately \$600 billion in 2001 to more than \$5,000 billion in 2005. The majority of all of this ecom- merce involves direct payment — 68% of 2001's volume and 80% of 2005's volume. IDC also projects that the B2B portion of this ecom- merce will grow more rapidly than the B2C portion. B2B ecommerce will increase from \$516 billion in 2001 to \$4,300 billion in 2005, a compound annual growth rate (CAGR) of more than 70%. This B2B

Copyright © 2002 IDC. Reproduction without written permission is completely forbidden.

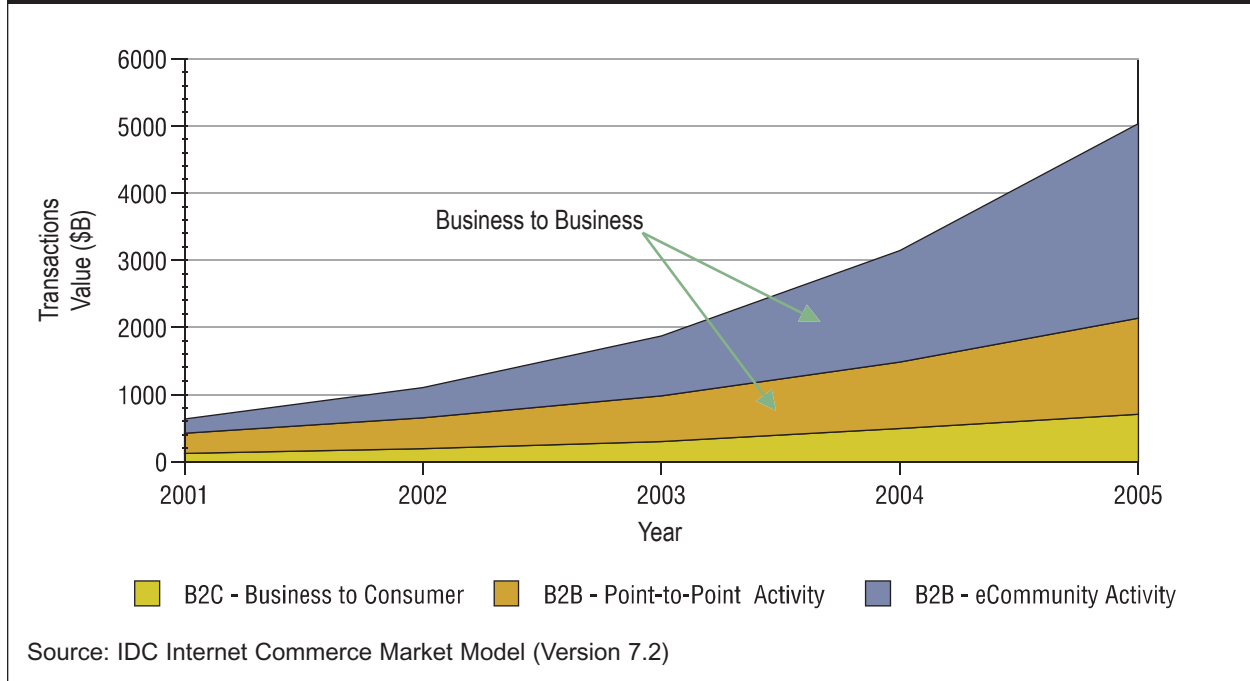
External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Printed on
recycled
materials



transaction volume occurs through various types of ecommunities as well as point-to-point transactions between individual businesses. illustrates each portion of that volume.

Figure 1
Worldwide eCommerce Transaction Volume, 2001-2005 (\$M)



TRUST IMPLICATIONS

As most industry commentators have pointed out, this level of direct ecommerce volume over public networks cries out for better security and protection. Much of the early growth in B2C and low-level B2B transactions leveraged the credit card infrastructure and model. The credit card approach, however, does not accommodate B2B volume and transaction size. New models must appear. Security companies, oversight agencies, and financial institutions have been claiming since the advent of the Web that the ecommerce marketplace needs a consistent, end-to-end secure infrastructure. As if to counter these predictions, ecommerce continues to grow without a secure infrastructure.

Security Optimization via Efficient Market Methods?

ecommerce transactions are already mushrooming without a specialized, complete, and integrated infrastructure. Does the market really need such a platform? Won't it find, on its own, the right balance of security and ease? Many entire markets and lead users have followed paths of "least resistance" to enable ecommerce. The mass market has leveraged open and widely available technologies to enable the boom to date. For example, because Secure Socket Layer (SSL) is easily deployed with most browsers, SSL "pipes" protect credit card and transaction information. Limited digital certificate public key infrastructure (PKI) implementations "verify" the legitimacy of key Web

Won't it find, on its own, the right balance of security and ease?

sites, and passwords remain the authentication means of choice if not perfection. Merchants seeking to exploit ecommerce grow to accept the cost to "cover" fraud as a cost of doing business on the Web.

These "security-lite" technologies remain popular while a host of broader security initiatives have faded from the market. Secure Electronic Transaction (SET), a payment card scheme and protocol driven by banks and vendors, has met with limited success. Many felt its complexity and expense overbalanced the fraud risk it countered. Likewise, many more advanced independent security technologies and alliances seem now to be fighting for coverage and share — with limited success. As the majority of businesses and the consumers they reach implement least-cost, lowest-overhead security approaches, a more robust security platform remains at the concept level.

The (Sublimated) Dark Side

The risks are real and growing.

But the risks are real and growing. Today's primary methods of protection are proving inadequate. The business impact and financial penalties for weak diligence are significant. *The 2001 Computer Crime and Security Survey*, commissioned by the Federal Bureau of Investigation, shows U.S. businesses suffering increasing financial losses as a result of computer crime and information security breaches. Only 186 of 500 survey respondents divulged financial losses, but even so, the losses totaled almost \$378 million. This compares to \$265 million in losses reported in 2000 by about 250 respondents.

eTailers experiencing chargeback rates of between 5% and 10%

Before the Internet stock bust, some electronic retailers (etailers), a large number of which are no longer in business, were experiencing chargeback rates of between 5% and 10% — a nonsustainable rate. A chargeback occurs when a cardholder disputes a credit card transaction and the card issuer works to resolve it with the merchant awaiting payment. Also, several well-publicized incursions resulted in thousands of card accounts becoming compromised. The published accounts mask a much wider problem since only a fraction of the security issues are noted and reported.

INSIDE BUSINESS-TO-BUSINESS TRANSACTIONS

The companies we spoke with recognized both the benefits of ecommerce and the risks described above. To assist us in framing the evolution of security technologies to support ecommerce, respondents provided a high-level view of the way they viewed high-risk transactions. They also shared how they expected to eventually protect those transactions over the public network. This closer look at the nature of B2B interactions helps frame the ultimate solution.

Most of these executives quickly pointed out the limits of IP-based ecommerce today. They pointed out the transaction domains ecommerce now touches and the substantial domains that it does not yet touch. In making these points, they consistently referenced four key points about B2B ecommerce. These issues point to the considerable lengths the IT industry must still travel to reach the robust levels of security essential for true ecommerce.

EDI never really did handle payments.

1. *Payments: A Different Kind of Transaction*

Bankers, merchants, and security infrastructure executives made pains to point out how little real payment transfers (as in transfers of actual currency and capital) occur over the public network, or even in the private networks extant before the Internet buildout. For example, electronic data interchange (EDI) evolved considerably from the mid '80s to the mid '90s, but during that entire period it never managed to incorporate the financial payment aspects of intercompany transactions. It remained a vehicle for "moving invoices," as one respondent put it.

The amount of "direct" ecommerce outlined above in IDC's ICMM model seems large. However, the actual funds transactions that support payment processes, such as credit cards and online banking, occur via proprietary leased line links or traditional wire transfers. For example, the actual transfer of funds from, for example, Wells Fargo to Nordstrom or from Fleet Bank to KeySpan, occurs from computer to computer over a private line — cumbersome and highly controlled options. In another example, the Federal Reserve is beginning to move some of its "ancillary" services out to the public network — for example, check adjustment functionality — however, it remains quite happy with its point-to-point, circuit-based, leased-line big bank connections for wire transfers.

2. *Sixty to Eighty Percent of the Value in 20% of the Transaction Volume Still Held Privately*

Actual payment and funds transfer transactions represent the top of the pyramid in terms of potential risk and requirement for security and trust. These remain controlled and private in part because fewer occur. That is, as the dollar value of transactions increases, the number of transactions of that type and size drop considerably. In a "reversed pyramid" effect, most transaction dollar volume occurs in relatively few large transactions — for example, a wire transfer of \$24 million between Bankers Trust and Deutsche Bank represents more volume than perhaps 10,000 other transactions. Figure 2 depicts this phenomenon.

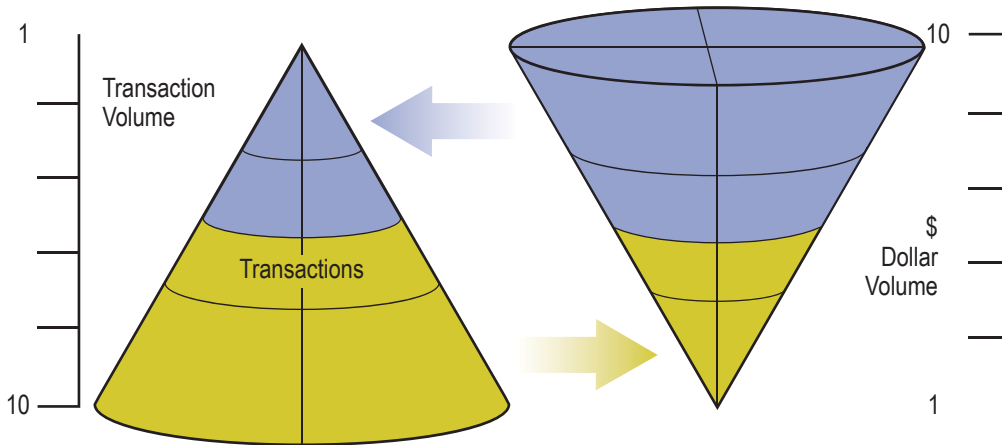
3. *Person-to-Person Trust and Honed Processes Enable the High-Value Transactions*

Research indicates that these "top-of-pyramid" transactions execute very efficiently across well-honed processes and with long-standing trust relationships between very large companies and institutions.

4. *We've Hardly Dented the Real Commerce Volume*

While we project 4,000 billion B2B ecommerce transactions in the entire year of 2005, the Federal Reserve does half that in wire transfers every day. Roughly \$2,000 billion changes hands via wire transfer every business day. Total commerce exchanges probably exceed that daily wire transfer number by 10 times, reaching 20,000 billion daily. We've hardly dented the real volume.

Figure 2
Business-to-Business Transaction Size and Transaction Volume



Source: IDC, 2002

APPLICATION FOCUS

In the context of these observations about real risk exposure, trust, and defined processes, IDC probed the interview group to understand how these enterprises plan to move higher-value transactions to the Web. Respondents indicated that in seeking to make their ecommerce processes more trustworthy and efficient, they consider security requirements and platforms on an application-by-application basis. They do not differentiate security requirements by transaction value. That is, rather than think of security for different transaction types and values within a business process, they think of the risk of the entire end-to-end application. Most indicated they then scaled the relative security requirements of their application portfolios across a multipoint risk assessment grid, presented as an example in Table 1.

Table 1
Application Security Risk Assessment Example

Factor	Measure	Examples
Information sensitivity	How would unauthorized release of this information affect people, institutions, markets, and so on?	Release of bank examiner data on Bank A's Asian loan portfolio could have, at one time, substantially affected markets, stocks, and economic investment.
Productivity impact	What business processes, services, or markets would this affect should it go down?	Stock trading exchanges Telecommunications network operations centers
Loss potential	How much money, resources, material, and so on, is exposed?	Wire transfers — exceptionally high potential; credit card purchases on Amazon.com — less so.

Source: IDC, 2002

In this context, leading organizations treat many nonfinancial transaction applications as respectfully, in terms of security support, as they do transaction systems. For example, hospitals responsible for maintaining patient record privacy set security policies for provider medical record exchange (a nonfinancial application) as tightly as they set policy for payroll fund transfer transactions and data. In the same way, the Federal Reserve Board may protect its online data service sites (e.g., rate information, currency valuations, etc.) much more assiduously than other enterprises protect their informational Web sites. This level of care reflects the loss in respect and trust that may ensue from a security breach or hacked site.

Transaction Security Requirements

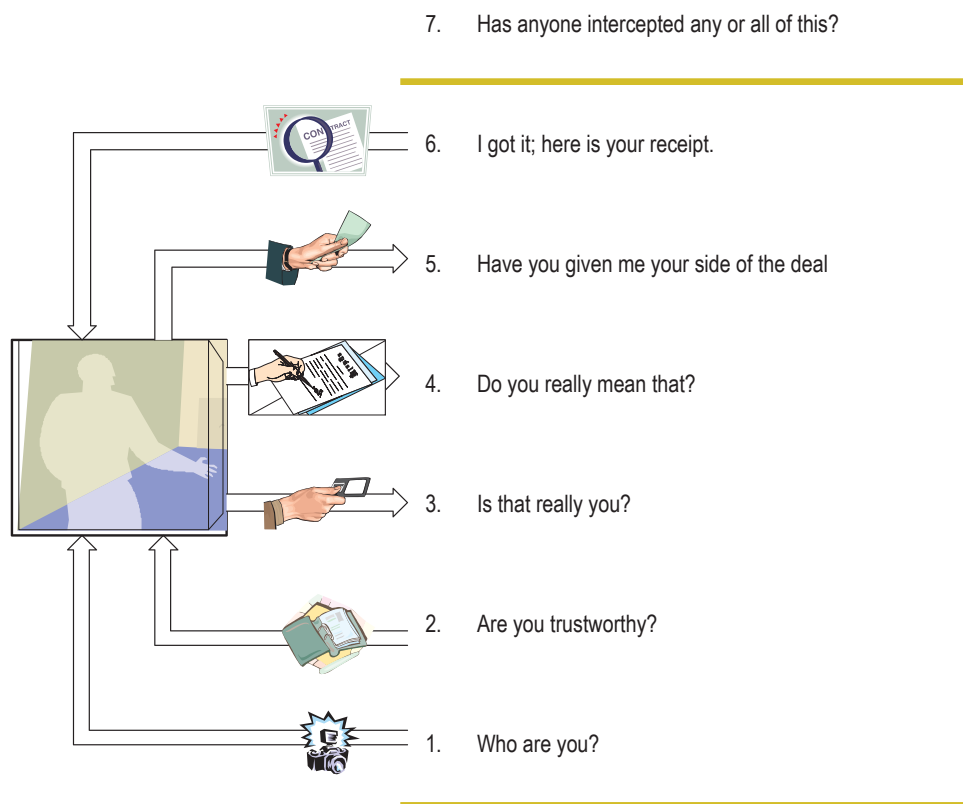
Within the context of this application perspective, most executives spoke of the need to replicate personal and physical trust parameters in the digital or ecommerce transaction. That is, executives indicated that they would begin porting applications to a TCP/IP Web-based infrastructure once they could assure that the application infrastructure provided the same or better trust.

To assess the trust implicit in any application platform, executives referenced many dimensions. Seven key components came up repeatedly as essential to their evaluation. Digital, Web-based versions of transaction applications need to meet each of these parameters unequivocally for trust to be assured. We depict these components in Figure 3 from the context of the party executing the transaction (financial, informational, or other). That party needs to know:

1. Who the other party to the transaction was — **Identify**
2. Whether that party could be trusted — for example, through a record or review or affirmation of his or her trustworthiness — **Assess**
3. Whether in fact the party at the other end of the transaction was indeed the party identified and assessed in items 1 and 2 — **Authenticate**
4. What the party wished to do (bid, obtain, buy, contract, etc.) and whether he or she really, legally meant to do it at this time — **Act**
5. Whether the party completed his or her side of the action/ transaction (e.g., transfer funds, transfer digital contract, etc.) — **Transmit**
6. Whether both parties can recognize the completed deal with a receipt or binding contract — **Confirm**
7. Whether anyone has eavesdropped on or intercepted any or all of these communications — **Assure Confidentiality**

While applications of different levels of sensitivity and risk demanded different degrees of redundant assurance for these trust components, all seven aspects need addressing.

Figure 3
Transaction Trust Parameters



Source: IDC, 2002

All of the respondents pointed to the wide gap between today's ecommerce trust infrastructure and the infrastructure that could support some of their most sensitive applications. They pointed to flaws and risks in today's environment that needed correction. Direct quote comments included the following:

- Eavesdropping (7) versus authentication (3) concerns: "... I don't worry as much about passwords being sniffed on the Internet as I do about access control to the password and authentication database."
- Consistent authentication (3), validation (4), confirmation (6): "... We need to validate the authenticity of the person doing the transaction at every single step of the way, not just once."
- Identification (1) and trustworthiness (2): "... It's hard to say that this [today's ecommerce infrastructure] is a solid thing. You have this example of Verisign and Microsoft."

"Hard to say that this today's infrastructure is a solid thing"

Respondent is referring to an incident where fraudulent certificates were issued to someone claiming to represent Microsoft.

"Our biggest challenge...emerging technologies"

- Identification (1), trust (2), and authentication (3): "... One of the requirements we have today is the identities that are issued ... to a hardware token. And that can be either in the end-user domain a smart card and at the server-side hardware security modules ... [It goes beyond the status quo but] that is a security component that allows us to maintain the integrity in the distributed network that we created."
- Scaling for authentication (3), act (4), transmit (5), and confirm(6): "... Our biggest challenge, quite frankly, was the fact that we had endeavored to use emerging technologies. And when I say that, I mean mostly around the security component, the public key infrastructure for large volume deployments."

The comments capture a tone that spoke clearly of the need to supply a more substantial, common, cross-certifiable infrastructure that could support the emerging world of ecommerce. Today's mix of independent Certificate Authorities (in some cases standalone), inconsistent checking of revocation lists, one-time-only validation checks, over-reliance on "pipe security" technologies such as SSL, and the extremely limited use of strong two-factor authentication — to name a few problems — need attention and revision. The market appears ready for a more comprehensive solution.

Building the Infrastructure Framework

Standardization, integration, and consistent deployment

A number of consortia and joint development enterprises are taking strides to fill the void and provide secure infrastructures. Their evolving efforts to build ecommerce frameworks, and the hurdles they face, may foretell the direction that the wider ecommerce industry must eventually take. The security technologies exist for effective infrastructures, but the standardization, integration, and consistent deployment await completion. Most of the joint development and consortia efforts reflect the immaturity of today's solutions.

Cross-certifying over 25 independent Certificate Authorities

One such effort, Identrus, seeks to provide the underlying trust infrastructure for the largest and most prestigious worldwide banks. Backed by the largest of commercial banks — which had worried about becoming "disintermediated" from the trust business by ecommerce — Identrus sought to build and provide a trusted platform for member banks and their B2B customers. The principal effort involved building a trusted hierarchy of digital IDs that each customer or bank could transfer and use among every other bank and customer. In this way, all banks and partners could be assured of trusted identity and authentication for procurement, bidding, ordering, paying, and other essential processes. Identrus spent considerable time and energy cross-certifying more than 25 independent Certificate Authority solutions for use by its target banks. At the time of the interview, the consortium had enlisted more than 40 of the largest of world banks. These, in turn, represented more than 50 million customers.

Identrus still considers the infrastructure in its early adoption stage, but it pointed to a myriad of emarketplaces and other applications its member banks and their customers were rolling out. Identrus continues to grapple with the challenges of pushing PKI to support

the volumes, high availability, and real-time response requirements of online business, but it is making progress. It also indicated that its approach to strong authentication (including requirements that all private keys for identity must be vaulted in a smart card, token, or protected hardware server device) has been paying dividends in very low fraud rates.

Identrus has made good progress toward its initial goal of increasing trust, identification, authentication, and validation service across its members. However, it seeks to go further. The organization will be taking on the risk of the member banks' and customers' end applications — such as Letter of Credit automation or insurance policy management — that operate on the Identrus infrastructure. As a final goal, it hopes to provide assurance for entire business processes that operate on its network.

The effort has demanded rigor, consistency, and interoperability from its vendor participants — especially the myriad security software companies providing a piece of the wide solution. It has likewise demanded strict policy adoption and compliance among its members — a price that most large financial institutions, including Barclays, Citibank, Bankers Trust, Deutsche Bank, and others, are willing and ready to take.

Similar, if less broadly adopted, infrastructure efforts are also under way. Cyber-COMM in France; E-cheque from the Financial Services Technology Consortium; SEMPER, an IBM-led European consortium; and a host of B2B communities — vertical market communities, portals, and so on — are trying to build in secure layers for trading activities.

*A model for the rest of the very wide
ecommerce community*

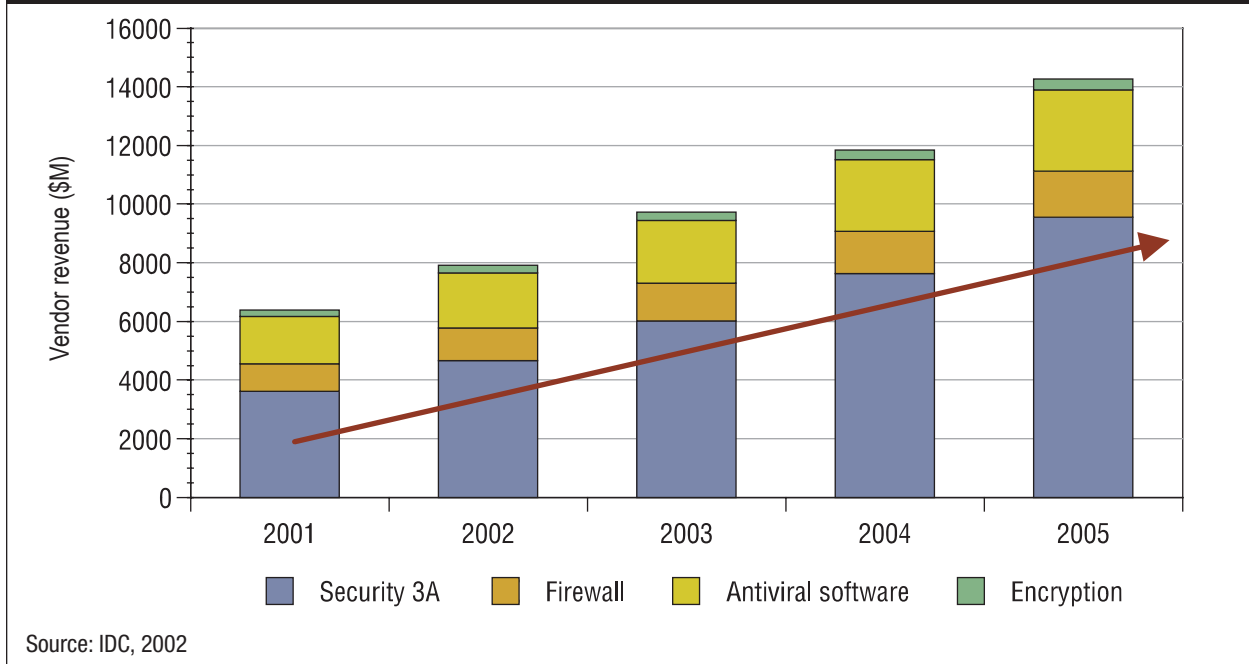
The Identrus example, coming as it does from the highest reaches of banking and ecommerce activities, may well serve as a model and harbinger for the rest of the very wide ecommerce community.

The Buildout Effect for Security Software Markets

In whichever fashion the ecommerce communities succeed and combine in providing the infrastructure, they must purchase and deploy a substantial amount of security technology to meet their objectives. Shakeout and consolidation notwithstanding, the security software market will grow substantially, reflecting the ecommerce buildout.

IDC forecasts strong growth for security, especially in the product segments most directly affecting ecommerce buildout. The so-called Security 3 As include product solutions for authentication, access control, and administration. Currently, more than 50% of the security market will grow faster than all other segments, reaching more than \$9.5 billion by 2005, at a 27% CAGR. The software security market will play a key role in this ecommerce buildout. Figure 4 presents IDC's forecast for overall security software market growth.

Figure 4
Internet Security Software Market Forecast



VALICERT AND ECOMMERCE SECURITY

A variety of transaction security solutions

The ValiCert Solution

ValiCert, a Mountain View, California, company, has been providing security solutions since 1996. It strives to help enterprises and service providers protect transactions throughout their life cycle. To these ends, ValiCert offers a variety of transaction security solutions that work with the customer's choice of Certificate Authorities, payment systems, and applications.

Initially, ValiCert focused on digital certificate validation. However, it has widened its solutions, adding a number of offerings that broaden its corporate focus. In its efforts to bring trust and legal standing to high-value and highly sensitive electronic transactions, ValiCert now offers not only the essential PKI and security technologies businesses need but also a wide range of software components to enable secure ecommerce.

This product line expansion enables ValiCert to offer solutions targeted to particular verticals such as finance, insurance, healthcare, and government. ValiCert is making strides to integrate its security solutions into industry solutions that target specific vertical needs.

These solutions are designed to streamline paper-based business processes, eliminating cost and time lags from key processes. They offer paperless solutions that assure delivery, pass legal requirements, leave complete audit trails, and prevent fraudulent repudiation.

*Trust Services, Validation Authority,
Digital Receipt Solutions, Document
and Transaction Authorities*

A Full-Solution Approach

The ValiCert infrastructure portfolio includes ValiCert Trust Services, ValiCert Validation Authority, ValiCert SecureTransport, ValiCert Digital Receipt Solutions, ValiCert Document Authority, and the ValiCert Transaction Authority. Its Core Managed Services are available to help speed up deployment of actual etransaction infrastructures. It also targets industries with special high-value transaction needs and wireless security.

Examples of ValiCert-enabled solutions span a number of industries. For insurance companies, ValiCert solutions can eliminate the Value Added Network (VAN) infrastructure costs insurance companies and banks normally incur when using leased lines or virtual private networking to handle high-trust transactions. The ValiCert SecureTransport solutions allow insurance companies to deliver sensitive content, such as health claims, securely even as they also take advantage of the lower-cost Internet. Using ValiCert SecureTransport and ValiCert Digital Receipt Solutions, these insurers can meet the privacy protection and audit trail requirements (that is, information about who has handled each transaction) that the Health Insurance Portability and Accountability Act (HIPAA) imposes. In moving to digital networked documents this way, insurance companies have replaced expensive, slow, and cumbersome paper-based processes.

For cross-border trade and finance, ValiCert provides essential document authority technology to wider solution providers such as Identrus, Bolero, and TradeCard. These combined solutions offer a low-cost digital means for replacing the very sensitive but costly and paper-prone Letter of Credit challenges rife in international trade and finance today.

Banking and financial services institutions face cost and speed issues with their traditional VAN infrastructures for sensitive corporate services such as cash management. ValiCert Trust Services and technology software coupled with wider consortium efforts, such as Identrus, offer financial-grade cryptography to allow banks to deliver secure, Web-based, cash management solutions to their corporate customers. ValiCert's Digital Receipt Solutions technologies provide assurance that only currently authorized personnel can access information and execute transactions.

CONCLUSION

The number of ecommerce transactions will continue to increase at robust rates throughout the world. However, trustworthy infrastructures that support the most sensitive and valuable of these transactions will require substantial buildout and consolidation. To date, we have seen the first generation of ecommerce security approaches. This generation has leveraged the bankcard model and certain "easy" and low-cost security components such as SSL. The next generation must support stronger identification, authentication, validation, and protection.

*Standardization, cross-certification,
and business cooperation enable the
next generation of ecommerce.*

We are seeing leading examples of this buildout in secure infrastructures such as Identrus' solution. These and other such efforts at standardization, cross-certification, and business cooperation for security will enable the next generation of ecommerce.

This next generation promises cost reductions in the form of reduced manual, paper-based processes; reduced reliance on proprietary electronic processes; and shortened business process cycle time. Effective, secure ecommerce will offer new revenue opportunities as well, empowering enterprises to offer innovative Internet-based products and services to a wider base of customers. Before enterprises truly embrace this next generation, they need assurance that they will not suffer hacker attacks, damage, and fraud. ValiCert's technologies, tied to wide-scale standard solutions, are addressing these key security hurdles.

However the buildout occurs, though, the market for software and components enabling that buildout will continue to grow at 20%-plus annual rates, presenting an opportunity for ValiCert and others offering the right solutions.

IDC Worldwide Offices

CORPORATE HEADQUARTERS

IDC
5 Speen Street
Framingham, MA 01701
United States
508.872.8200

NORTH AMERICA

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario M5C 2C5 Canada
416.369.0033

IDC California (Irvine)
18831 Von Karmen Avenue
Suite 200
Irvine, CA 92612
949.250.1960

IDC California (Mountain View)
2131 Landings Drive
Mountain View, CA 94043
650.691.0500

IDC New Jersey
75 Broad Street, 2nd Floor
Red Bank, NJ 07701
732.842.0791

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212.726.0900

IDC Texas
100 Congress Avenue
Suite 2000
Austin, TX 78701
512.469.6333

IDC Virginia
8304 Professional Hill Drive
Fairfax, VA 22031
703.280.5161

EUROPE

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
Vienna A-1040, Austria
43.1.50.50.900

IDC Belgium
Boulevard Saint Michel 47
1040 Brussels, Belgium
32.2.779.4604

IDC Denmark
Omøgade 8
Postbox 2609
2100 Copenhagen, Denmark
45.39.16.2222

IDC Finland
Jarrumiehenkatu2
FIN- 00520 Helsinki
Finland
358.9.8770.466

IDC France
Immeuble La Fayette 2
Place des Vosges Cedex 65
92051 Paris la Defense 5, France
33.1.49.04.8000

IDC Germany
Nibelungenplatz 3, 11th Floor
60318 Frankfurt, Germany
49.69.90.50.20

IDC Italy
Viale Monza, 14
20127 Milan, Italy
39.02.28457.1

IDC Netherlands
A. Fokkerweg 1
Amsterdam1059 CM, Netherlands
31.20.6692.721

IDC Portugal
c/o Ponto de Convergancia SA
Av. Antonio Serpa 36 - 9th Floor
1050-027 Lisbon, Portugal
351.21.796.5487

IDC Spain
Ochandiano, 6
Centro Empresarial El Plantio
28023 Madrid, Spain
34.91.7080007

IDC Sweden
Box 1096
Kistagangen 21
S-164 25 Kista, Sweden
46.8.751.0415

IDC U.K.
British Standards House
389 Chiswick High Road
London W4 4AE United Kingdom
44.208.987.7100

LATIN AMERICA

IDC Latin America
Regional Headquarters
8200 NW 41 Street, Suite 300
Miami, FL 33166
305.267.2616

IDC Argentina
Trends Consulting
Rivadavia 413, Piso 4, Oficina 6
C1002AAC, Buenos Aires, Argentina
54.11.4343.8899

IDC Brazil
Alameda Ribeirao Preto, 130
Conjunto 41
Sao Paulo, SP CEP: 01331-000 Brazil
55.11.3371.0000

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 13
Providencia
Santiago, 9, Chile
56.2.334.1826

IDC Colombia
Carerra 40 105A-12
Bogota, Colombia
571.533.2326

IDC Mexico
Select-IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo Condesa
C.P. 06100, Mexico
525.256.1426

IDC Venezuela
Calle Guaicaipuro
Torre Alianza, 6 Piso, 6D
El Rosal
Caracas, Venezuela
58.2.951.1109

CENTRAL AND EASTERN EUROPE

IDC CEMA
Central and Eastern
European Headquarters
Male Namesti 13
110 00 Praha 1
Czech Republic
420.2.2142.3140

IDC Croatia
Srednjaci 8
1000 Zagreb
Croatia
385.1.3040050

IDC Hungary
Nador utca 23
5th Floor
H-1051 Budapest, Hungary
36.1.473.2370

IDC Poland
Czapli 31A
02-781 Warszawa, Poland
48.22.7540518

IDC Russia
Suites 341-342
Orlikov Pereulok 5
Moscow, Russia 107996
7.095.975.0042

MIDDLE EAST AND AFRICA

IDC Middle East
1001 Al Ettihad Building
Port Saeed
P.O. Box 41856
Dubai, United Arab Emirates
971.4.295.2668

IDC Israel
4 Gershon Street
Tel Aviv 67017, Israel
972.3.561.1660

IDC South Africa
c/o BMI TechKnowledge
3rd Floor
356 Rivonia Boulevard
P.O. Box 4603
Rivonia 2128, South Africa
27.11.803.6412

IDC Turkey
Tevfik Erdonmez Sok. 2/1 Gul
Apt. Kat 9D
46 Esentepe 80280
Istanbul, Turkey
90.212.275.0995

ASIA/PACIFIC

IDC Singapore
Asia/Pacific Headquarters
80 Anson Road
#38-00 IBM Towers
Singapore 079907
65.226.0330

IDC Australia
Level 3, 157 Walker Street
North Sydney, NSW 2060
Australia
61.2.9922.5300

IDC China
Room 611, Beijing Times Square
88 West Chang'an Avenue
Beijing 100031
People's Republic of China
86.10.8391.3610

IDC Hong Kong
12/F, St. John's Building
33 Garden Road
Central, Hong Kong
852.2530.3831

IDC India Limited
Cyber House
B-35, Sector 32, Institutional
Gurgaon 122002
Haryana India
91.124.6381673

IDC Indonesia
17th Floor, Tower 2
Jakarta Stock Exchange
Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
62.21.515.7759

IDC Market Research (M) Sdn Bhd
Jakarta Stock Exchange Tower II
17th Floor
Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
62.21.515.7676

IDC Japan
The Itoyama Tower 10F
159-1, Samsung-Dong
Tokyo 108-0073, Japan
81.3.5440.3400

IDC Korea Ltd.
Suite 704, Korea Trade Center
159-1, Samsung-Dong
Kangnam-Ku, Seoul, Korea, 135-729
822.551.4380

IDC Market Research (M) Sdn Bhd
Suite 13-03, Level 13
Menara HLA
3, Jalan Kia Peng
50450 Kuala Lumpur, Malaysia
60.3.2163.3715

IDC New Zealand
Level 7, 246 Queen Street
Auckland, New Zealand
64.9.309.8252

IDC Philippines
703-705 SEDCCO I Bldg.
120 Rada cor. Legaspi Streets
Legaspi Village, Makati City
Philippines 1200
632. 867.2288

IDC Taiwan Ltd.
10F, 31 Jen-Ai Road, Sec. 4
Taipei 106
Taiwan, R.O.C.
886.2.2731.7288

IDC Thailand
27 AR building
Soi Charoen Nakorn 14,
Charoen Nakorn Rd., Klongtsonai
Klongsan, Bangkok 10600
Thailand
66.02.439.4591.2

IDC Vietnam
Saigon Trade Centre
37 Ton Duc Thang Street
Unit 1606, District-1
Hochiminh City, Vietnam
84.8.910.1233; 5

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and ebusiness trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, ebusiness companies and the financial community. Additional information can be found at www.idc.com.

IDC is a division of IDG, the world's leading IT media, research and exposition company.

02C3182VALICE3182
February 2002

