Gartner

A White Paper Prepared for

Verisign, Inc.

The Evolution of e-Business Security Requirements

Engagement: 220011370

Gartner Consulting

251 River Oaks Parkway, San Jose, CA 95134-1913
+1-408-468-8811

Table of Contents

Introduction

The growth of the Internet in the past ten years has been phenomenal. Companies, large and small, have embraced the Internet as a tool that can potentially expand their businesses beyond traditional boundaries and perhaps give them a competitive advantage in the marketplace. For example, Gartner estimates that nearly 14 percent of business-to-business payments are currently made electronically, with that number expected to grow to over 50 percent by the year 2009. All of this hype is leading to enormous pressure on managing directors, CEO's and CIO's to create and implement e-business solutions now, if not sooner.

One question these executives will encounter in considering their company's Internet strategy is that of security. From the executive's vantage point, yes!, the potential revenue generation and cost savings to my business provided by the Internet are significant, but what do I do to ensure the security of this activity against possible fraud, theft, or Internet vandalism?

One aspect of e-business is that the sheer volume of commerce on the Internet requires a more robust and efficient method of verifying the identity of the person with whom one is doing business and protecting sensitive information. The 25-year-old technology of public key cryptography (PKC) fills the need for a commercially applicable means of verifying identity and managing encryption. Helping to facilitate this need, powerful servers support the processing of large-scale certification services, hardware accelerator process digital signatures in a fraction of the time needed by a software package, and telecommunications services support the bandwidth needed for a wave of certificate requests and standards have been published for many of the requirements.

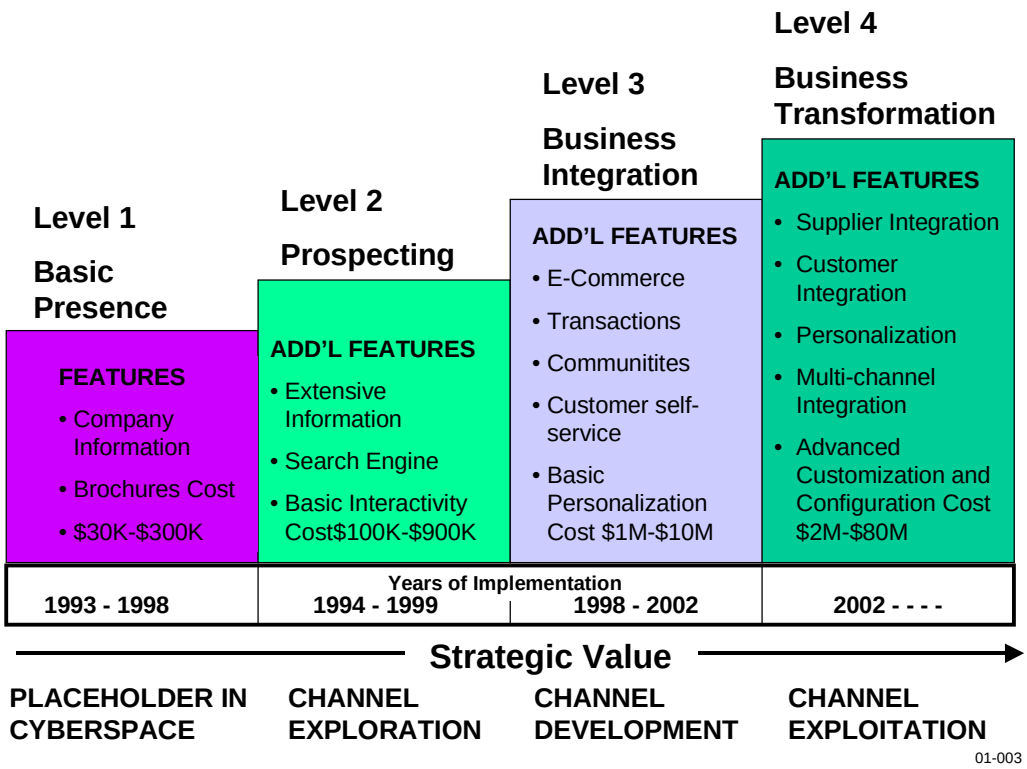
This white paper discusses the evolution of the Internet as a business tool, with specific focus on the importance of public key infrastructure (PKI) as an integral part of Internet security. Topics of note include:

- The evolution of the Internet as a strategic business tool, e-business
- The parallel evolution of Internet Security
- Options for securing e-business including a roadmap for a successful PKI implementation
- A case study example.

The Evolution of the Internet as a Strategic Business Tool

The initial use of the Internet as a business tool was predominantly for marketing purposes in the form of a public information Web site. Companies now leverage their Web sites for product support, customer service, and retail sales and as a delivery channel for electronic goods and services. The overall result is that the cost, sophistication and business value of Web sites for most industries has grown dramatically in the last three years. The next three years will see even greater growth in value and associated cost. The importance and complexity of the Web as a business tool is best illustrated in the figure below, defined as the Gartner Enterprise Framework for Strategic Websites.

Figure 1: Gartner Enterprise Framework for Strategic Websites.



Source: Gartner (2000)

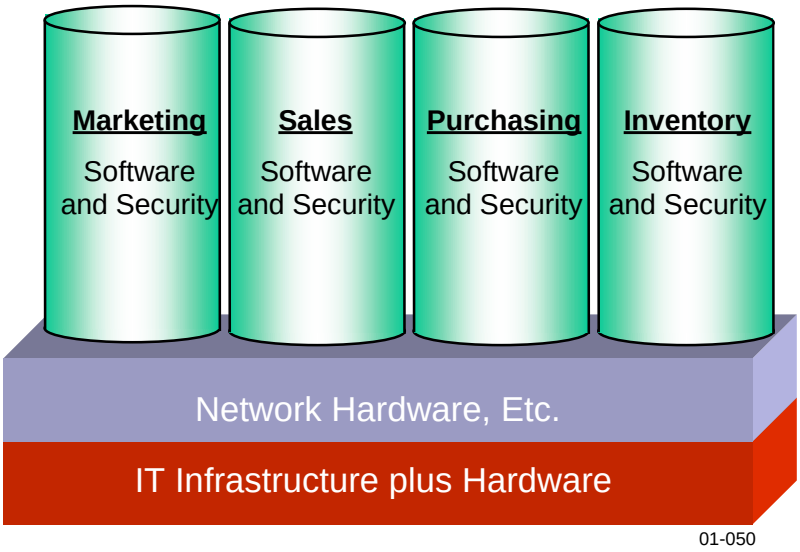
As the figure shows, the web has gone from a passive, advertising tool, to one that integrates all functions of a company's business. This integration has also meant that the undertaking of an e-business initiative is no longer just an IT issue.

No Longer Just an IT Issue

True e-business, as defined by Gartner, incorporates IT infrastructure, networks and applications for continuous optimization of its value chain position. In summary, e-business is the evolution of the enterprise. This concept is graphically presented in Figure 2 below:

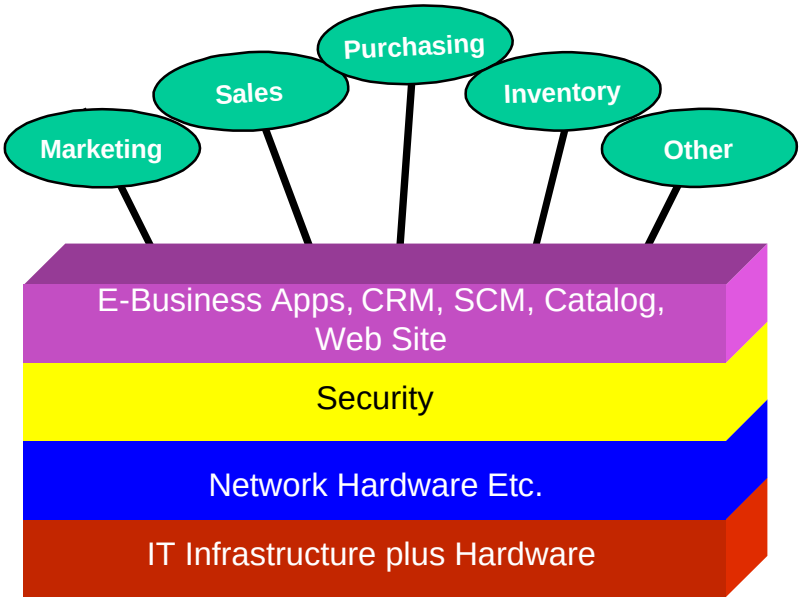
Figure 2: Evolution of the Enterprise

Enterprise Without E-Business Integration



Source: Gartner 2001

Enterprise With E-Business Integration



Source: Gartner 2001

When a firm decides to implement an e-business initiative, it must realize the depth of work that it is undertaking. From the CEO down to the mailroom clerk, business processes are reevaluated so that the focus is no longer just on cost reduction, but towards a more externally-focused business strategy. In addition, individual company functions such as marketing, finance,

purchasing, etc. can no longer operate as independent silo organizations. The resulting enterprise integration of a company's resources confirms that e-business is no longer just an IT issue. This strategy has a goal of creating a customer-focused, agile supply and demand chain capability that drives revenue generation.

One example of a company successfully reaching Level 4 (Business Transformation) is Cisco Systems, Inc. With a goal of generating over 90 percent of its total sales over the Web, Cisco has fully embraced the Internet as a business tool. Cisco has defined its website as Cisco Connection Online (CCO), whose primary focus is to deepen customer relationships with existing customers, reduce cycle time, lower costs, and promote sales. A FY2000 Cisco study showed overall CCO-related savings of over $500 million annually, including reduced call center volume, shipping cost, and other expenses. Cisco's success has been realized by successfully leveraging the power of the Internet.

In summary, this new e-business initiative focuses as much on external processes as internal, and success is measured in financial impact to the business, not only in efficiency metrics. Of course, e-business initiatives driving this integration of resources has also meant that the need for Internet security has also had to evolve in parallel.

The Evolution of Internet Security-An Introduction to Levels One and Two in the Gartner Framework

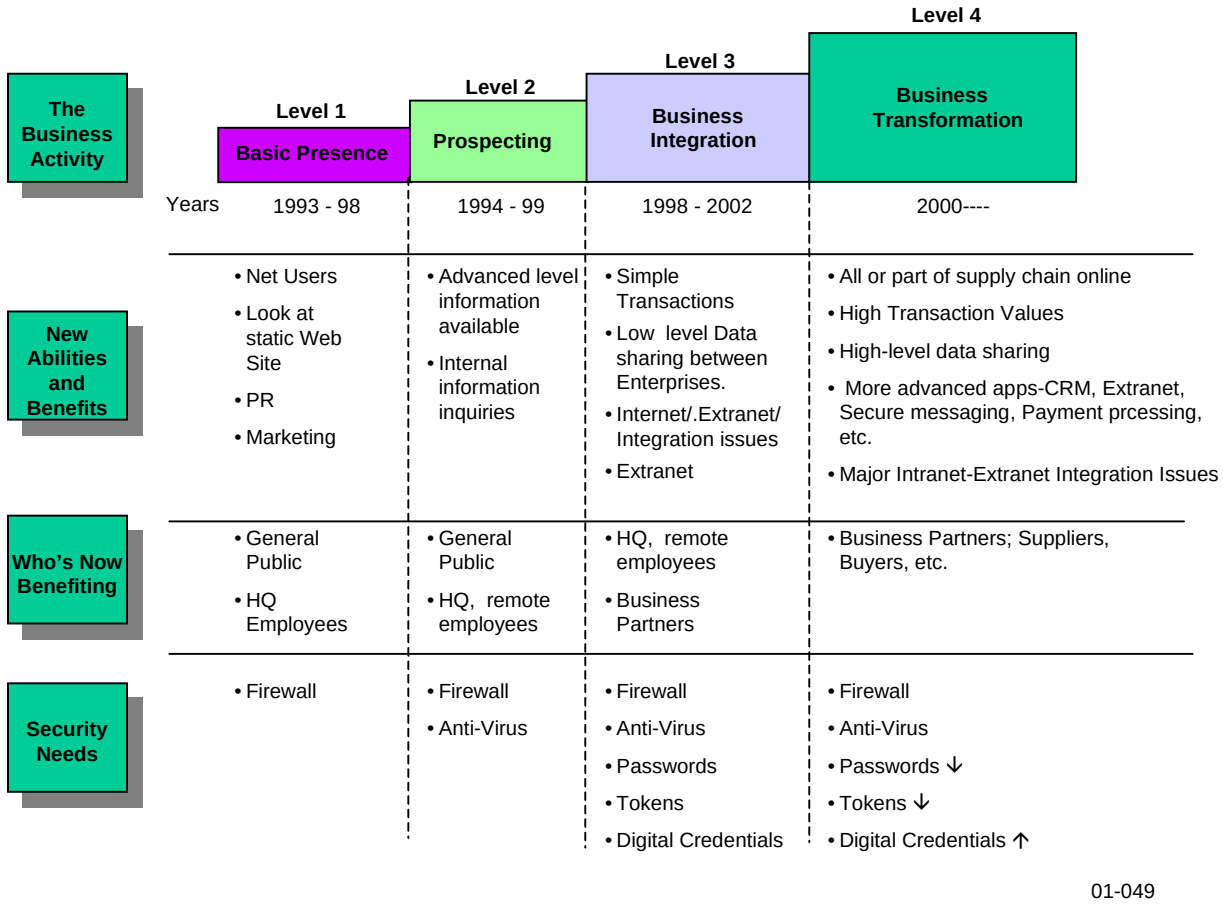
For many companies, the initial attempt to capitalize on the Internet was to invoke level one of the strategic framework shown in Figure 1. This low-level strategy gave the company a placeholder in cyberspace and was really just a simple extension of the marketing communications department.

This simple web presence also made it necessary for a company to open its network to potential security breaches. An answer to this security concern was the advent of firewalls. Early firewalls had simple objectives:

- Prevent unauthorized external users from accessing the enterprise network
- Allow Internet email and web surfing.

As Figure 3 graphically represents, the use of the Internet for e-business continues to ramp up and many companies move through levels two through four in the strategy framework, the Internet Security answer no longer is the implementation of a simple firewall. In each succeeding level, transactions typically increase in value and include not just monetary transactions, but may also include valuable information such as intellectual property. With such high-valued transactions, companies need higher levels of security to protect themselves.

Figure 3: As the Enterprise Evolves towards E-Business, so do the Security Needs



Source: Gartner 2001

Given that a company is in fact moving toward the external, extranet-focused Levels 3 and 4, what are the new security risks that need to be managed, and what other security mechanisms besides firewalls, and anti-virus protection, must the enterprise deploy? The answer is the risks include:

- User authentication
- Application access, and transaction level authorization and electronic signatures (could be called authority
- Validation approval.

The choices for managing these risks are Passwords and Digital Certificates.

Ascending to Levels Three and Four in the Gartner Framework: Building Trust with Your Stakeholders

Authentication:	Proofs and credentials verify the process by which an identity claimed by or for a user or other system entity.
Authorization:	The process, which determines what resources a user may access and what, they may do with them.

As an enterprise strives to attain either Level 3 (Business Integration) or Level 4 (Business Transformation) within the Gartner Strategic Framework, the issue of **WHO** can access the system and **WHAT** they can do once they have access becomes a key issue. Do you know that the entity claiming to be a business partner can be trusted and if so, what will you allow that entity to do once they are in? Will that entity have access to purchasing records, the ability to review open bids, etc? An authentication schema helps answer the who question, while the question of what is answered by authorization.

Successfully authenticating a user establishes his or her identity, and all activity under that identity is tracked, thereby making the user accountable for the activity — hence, the need for management practices over the authentication information. PINs or passwords are currently the standard user authentication solutions, both on the Internet and for internal applications. PINs typically control access to personal information, (e.g., bank account information), while passwords are used to control access to personal information as well as shared information, such as sensitive or trade secret information contained in data files.

Authorization can be established by permissions or access rights—such as read, write and update—associated directly or indirectly with the user ID and with the electronic content. As users have leveraged the encryption native to browsers and deployed encrypted IP stacks, they have found that access control lists (ACLs) located on each target server can become a management nightmare as more servers are deployed. While security people talk about authorization, marketers and business managers talk about personalization and one-to-one marketing. Authorization is expected to be driven by personalization mechanisms to answer this need.

In simple terms, authentication and authorization can be described by the use of the international travel analogy. For example, traveling from country to country requires a passport, which is accepted to **authenticate** the identity and citizenship of the bearer because it was attested to by a trusted third party. Now if the bearer of the passport wants to enter a specific country, that country would typically need to issue the traveler a visa. The issued visa gives the traveler **authorization** to enter to and travel within a specific country.

For authentication purposes, although passwords and tokens may be adequate to an extent, digital certificates can add an extra level of security. Issues with only using passwords and tokens can include:

- Low-level of security
- High-cost

- Non-scaleability
- Short lifespans
- Lack of an ability for non-repudiation.

At levels 3 and 4, the value and number of business transactions can increase dramatically. Organizations are beginning to choose the use of e-signatures as a solution in order to speed transactions, save costs, reduce paper, and in many cases, to improve transaction security. In simple terms, an e-signature can be defined as the following:

"The electronic equivalent of the handwritten signature or "wet" signature"

The so-called U.S. "E-Sign" law—gives e-signatures on contract the force of law. The most full-featured and, arguably, the most secure type of e-signature, is the digital signature, which relies on PKC to authenticate identity. Therefore, attaining the needed level of trust for levels 3 and 4 is possible within the context of a well-designed PKI. The digital certificates created by the certification authority permit trusted electronic relationships inside and outside the organization with consumers, suppliers, and business partners. Thus, PKI can be an important technology in enabling e-business.

The Role of PKI

PKI is not simply an authentication technology. When there is a risk of fraud, a risk of legal ramifications if a transaction is altered or disclosed, or when the confirmed identity of an individual or business entity is essential, PKI becomes crucial. For this reason, organizations in finance, government, health care, e-business, and manufacturing are well positioned to consider implementing PKI.

Other critical functions and benefits that PKI provides include:

- **Confidentiality**, which protects sensitive information
- **Integrity**, whereby transactions are guaranteed not to be altered
- **Non-repudiation**, which provides evidence that transactions have occurred
- **Integration,** the ability to integrate with all company functions, marketing, sales, finance, etc., rather than through a piecemeal integration process.

PKI provides the tools to manage public and private keys that, among other things, can be used to authenticate the holder of the private key, assuming the user has protected the private key and has it when it is needed. To date, this has relegated PKI to mostly prototype use as businesses struggle to find applications with enough business benefit to justify the investment required to overcome these barriers. However, smart cards will gain more widespread use and therefore provide security and portability and will be an enabler to more widespread use of PKI in the future. A key driver will be the need for businesses to trust the identity of the individual on the other side of an e-business transaction.

In the interim, Gartner believes communities of interest will be able to make effective use of PKI as the technology becomes more embedded in applications and operating systems.

Organizations that are considering a PKI implementation should evaluate the following:

- What types of industry are they in?
- What is the existing information security infrastructure
- What types of transactions are occurring?
- What is the sensitivity of the transactions taking place?
- What is the level of in-house/organizational expertise?
- What is the willingness of the organization to commit in-house resources?

Pulling it all Together: A Road Map For PKI's Role in Internet Security

The selection of PKI vendors, products, or approaches should take place within the context of a full security plan in the organization. The plan should take into account the results of risk analysis and should include a formal written security policy. Because the purpose of the PKI is to enable the business to conduct essential transactions safely over insecure networks, the demands of the business will determine the key factors for operation and performance.

General business requirements to be considered when implementing a PKI solution include:

- The need to make the certificate authority (CA) accessible to the Internet, intranet, and/or extranet
- The need to show in the certificate the extent to which the CA verified the identity of the user of the certificate and any authority (such as the capability to place purchase orders up to a specified value) associated with them
- The frequency of adding certificates
- The frequency of revoking certificates. Some sources recommend checking for frequency of suspending certificates; in practice, certificate suspension is quite rare and still very conceptual
- Other PKI users monitoring the impact on the server and telecommunications connections will make how often checks on issued certificates
- Legal liability associated with the certificates
- The cost of integrating PKI technologies into the business applications that is enabled by the PKI.

Insource vs. Outsource

While most cost discussions around PKI deal with deploying a PKI within an organization, the alternative of hosted or outsourced PKI services exists. It's a classic, build or rent, situation with cost advantages and disadvantages for each option. Deploying a PKI within the organization (build) requires up-front costs for equipment, consulting, training, and testing. However, the cost per certificate will go down significantly as the system is used. On the other hand, outsourced

PKI (rent), as with any other outsourced function, is cheaper to set up initially but remains at roughly the same cost level over the months and years. Once it is set up, there are no incremental costs and it can be used repeatedly.

Many clients choose a hybrid build or rent solution wherein they can outsource parts of the PKI that are infeasible to profitably build and maintain in-house, while at the same time internally developing and maintaining those parts of the PKI that they consider strategic. Each organization that opts for PKI will select a mix of build and /or buy that best reflects its overarching strategic concerns and capabilities.

Since most IT staff members have little experience with PKIs, the risk of expensive mistakes is very real. It would be worthwhile to work with a vendor or consultant with a great deal of experience creating PKIs for the buyer's size and type of organization. The major PKI vendors offer extensive consulting services and implementation packages. Therefore, the price of consulting, implementation, and training must also be taken into account.

Looking Towards the Future

The "XML-ing" of PKI: As XML is adapted to describing business logic, it is being applied to information security and PKI. The goal is to apply security and PKI functions to those portions of documents that logically benefit from it or where it is required, rather than encrypt or sign complete documents, coding included. For example, e-forms may call for a signature on a portion of a document that approves a transaction, whereas the entire form may be signed by another entity to verify that nothing was changed on the template. In another case, vendors are looking to bring certificate-handling routines to XML-based applications to subsume current toolkit-added functionality such as requests, certificate submittals and validations based on the Certificate Management Protocol, Certificate Management System, PKCS #7 and #10, and vendor proprietary methods. As we enter this phase, the risk is market confusion over rapid-fire, multiple and overlapping XML developments. Because these specifications will tend to be inexact, developer interpretation can cause interoperability problems.

XML does have momentum for describing Internet documents and providing inter-application functionality; therefore developer adoption of XML security methods is desirable. Looking towards the future, user organizations must insist on interoperability demonstrations from their vendors and internal developers, despite any nuances or interpretations made to the specifications prior to their being locked into formalized standards.

The potential benefits of combining XML with PKI could include:

- No need to delay PKI deployment pending client support, as the XML Key Management Specification (XKMS) moves the complexity of PKI and trust processing to server-side components instead.
- Being future proof against new PKI developments, as application developers benefit when the impact of future PKI developments is restricted to server-side components.
- Allowing mobile devices to access full-featured PKI through ultra-minimal footprint client interfaces.

These potential benefits would be contingent on the XKMS open standard being able to deliver on the promise of enabling applications to make trust service requests directly to trust service providers.

Case Study

A U.S. Headquartered International Financial Institution

Objectives:

From an IT infrastructure and security perspective, it was determined that it was a priority to find a process to allow its commercial customers to access banking applications. The decision was made to implement PKI first as an external project, focusing on customer-facing applications and potentially migrate the process internally for its over 70,000 worldwide employees.

Key Issues:

An IT Director working on e-business issues and related banking matters, realized that PKI could potentially facilitate business and build trust with retail customers. Passwords and ID's were currently being used, but not viewed as a long-term security solution for authentication. A small group decided to do a pilot program that would work with retail online banking applications.

The Process:

The initial phase of the project dealt with building an authentication process for an online banking system. From the outset, an underlying belief was that PKI is not just about technology, but about the rules around the technology. This mindset made vendor selection and the implementation partner selection critical. The implementation partner was defined as the entity (often Big 5 Accounting Firm) that would assist the client in writing the certification practice statements (CPS) and certificate policies (CP).

A proof of concept PKI pilot project was then developed for the retail online banking system. It was later determined that, because of financial and organizational constraints, it was not feasible to rollout PKI for the retail sector, but the work that had been completed was seen as leverageable for the commercial sector. Buy in from top management has allowed PKI to now be used primarily in business to business (B2B) processes ranging from currency trading applications, to domestic check clearing applications.

Key deliverables for the PKI implementation included:

- Working with a vendor who had an onsite product which allowed the client to do all of the registration in-house, yet not necessitate large capital outlays to build an onsite secure building.
- Going forward, a vendor who would be able to scale with the client as business processes, and hence PKI needs, expanded. Scalability was important as the client was expecting to add more commercial banking applications to its portfolio and was potentially undergoing a merger.

- Ability to capitalize on the e-sign legislation, which allows for digital signatures on documents that, are contractually of high-value or of a transactional nature.
- Ability to migrate PKI from external processes and applications to internal ones, one potentially being internal email systems.

Conclusion

The Internet's use as a business tool can have a dramatic effect on the management of an enterprise. E-business is not simply a monetary transaction that happens over the Internet, but a much more complex exchange of data ranging from contractual data from both customers and suppliers to internal company data for "Internal Use Only" purposes. In addition, a company's decision to undertake an e-business initiative is no longer just an IT issue and has evolved far past the point of just being a billboard posted in cyberspace. The e-business initiative requires that the enterprise integrate:

- E-commerce
- Customer relationship management
- Knowledge management
- Supply chain and logistics management applications
- Value chain processes
- Business partners' processes.

The integration of the above processes makes it imperative that all stakeholders participate in the creation and definition of enterprise security as it relates to e-business. This will diminish gaps in security as well as ensure the seamless participation of the stakeholders. It is this seamless participation from all groups within the enterprise that leads to a streamlined organization, thus cutting expenses and redundancies. PKI as part of a total enterprise security solution can help facilitate this business process transformation.

The Bottom Line

As stated earlier in this paper, PKI becomes crucial when there is a risk of fraud, a risk of legal ramifications if a transaction is altered or disclosed, or when the confirmed identity of an individual or business entity is essential. The features of the leading PKI products are very similar, although deployment models differ, with some offering services and the others offering product for the enterprise to operate. Enterprises must decide; in cooperation with their trading partners, at what level and how many registration authorities (RAs) and CAs will operate. And use those assumptions in conjunction with the selection criteria described in this white paper to pick the product or service that best meets their immediate needs for increased e-business security. To reiterate, key issues in evaluating a vendor would include:

- The vendor's ability to assist the client in understanding the build or rent decision and to deliver an appropriate solution based upon the client's stated and unstated needs.
- The vendor's ability to effectively assist the client in enterprise application integration (EAI) at each step.
- The vendor's ability to provide a scalable solution as the client company grows.

- The vendor's ability to provide authentication and authorization functionality as part of he defined security solution.

A vendor who is able to offer these software tools and integration services can truly help their customers leverage the power of the Internet for e-business.