DIGITAL SIGNATURE: APPLICATION DEVELOPMENT TRENDS IN E-BUSINESS

Parag Shiralkar
Management Department
The University of Akron
sparag@uakron.edu

Bindiganavale S. Vijayaraman
Management Department
The University of Akron
vijay@uakron.edu

ABSTRACT

Applications of digital signature technology are on the rise because of legal and technological developments, along with strong market demand for secured transactions on the Internet. In order to predict the future demand for digital signature products and online security, it is important to understand the application development trends in digital signature technology. This comparative study across various modes of e-business indicates that the majority of digital signature applications have been developed for the Business-to-Business (B2B) mode of e-business. This study also indicates a slow adoption rate of digital signature products by governments and the potential for their rapid growth in the Business-to-Consumer (B2C) mode of e-business. These developments promise to provide a robust security infrastructure for online businesses, which may promote e-business further in the future.

Keywords: Digital Signature, E-business, Secure Business Processes

1. Introduction

Rapid developments in e-business pose a growing need for online security and authentication. Many emerging technologies are being developed to provide online authentication. The major concern in e-business transactions is the need for the replacement of the hand-written signature with an 'online' signature. The traditional e-mail system, which has problems of message integrity and non-repudiation, does not fulfill the basic requirements for an online signature. Further, since the Internet communication system is prone to various types of security breaches, the discussion of robust and authenticated e-business transactions is incomplete without consideration of 'security' as a prominent aspect of 'online signatures'. One may consider an e-signature as a type of electronic authentication. Such authentication can be achieved by means of different types of technologies. A Digital Signature (DS) can be considered as a type of e-signature, which uses a particular kind of technology, that is DS technology.

DS technology involves encrypting messages in such a way that only legitimate parties are able to decrypt the message (Gelboard, 2000). Two separate but interrelated 'keys' carry out this process of encryption and decryption. One party in the transactions holds the secret key, or the private key, and the other party holds the public key, or the key with wide access. The selection and use of an encryption technique plays a crucial role in the design and development of keys. In short, a DS satisfies all the functions, such as authenticity, non-repudiation, and security, of a hand-written signature. Such a 'signature' can be viewed as a means of authentication and can be owned by an individual. While using this technology, there must be third party involvement in order to handle the liability issues that may be raised by bilateral transactions. The Utah Digital Signature Act introduced the concept of a Certifying Authority (CA), which acts as a trusted third party (Utah Department of Commerce, 1994). After the Utah Digital Signature Act was enacted, many other states either implemented similar e-signature acts or had some clause associated with security and online authentication added to their state laws. Furthermore, the federal Global and National Commerce Act provided equal authenticity to both hand-written signatures and e-signatures (Wright, 2000). This technologically neutral act was intended to promote e-business applications in all its modes such as business-to-business (B2B), business-to-consumer (B2C), and business-to-government (B2G). With this existing legal infrastructure and the rapid emergence of software security products, it is important to understand the role of emerging technologies like DS in e-business. One of the major indicators of technological improvements is the market development and commercialization of that technology. This paper focuses on the application development trends in DS technology for e-business. The data were gathered from business news reports that described DS products. The results focus on the analysis of industry and application trends in the use of DS technology. This paper

also provides insight into varying needs for DS products across different modes of e-business and the market response to these needs.

2. Overview of Digital Signature Technology

The application of DS requires technical infrastructure in the form of public/private keys, software that integrates user applications with the encryption process, and the necessary hardware required for the operation. DS infrastructures are usually developed for a specific area of technology. Some companies have developed Public Key Infrastructure (PKI), which provides solutions for the DS application and security. The Certifying Authority (CA) who issues a Digital Certificate (DC) to a customer also works as a service provider for different DS technologies. One such service provider, IDCertify Inc., provides technical infrastructure and solutions for DS applications. The signatures are verified with the help of licensed and audited test centers all over the world (IDCertify, Inc., 2002). Another leading CA service provider is Verisign Inc., which primarily works in the area of retail and enterprise services. Its services include providing PKI infrastructure depending on the requirements of an enterprise, and also include consulting and training services. Most of the security services offered by Verisign Inc. are based on a 128-bit encryption process (Verisign, Inc., 2002). Another service provider, Globalsign, Inc. creates and manages DCs for signed and sealed e-mail messaging for secure and confidential e-commerce and m-commerce applications (Globalsign, Inc., 2002). The availability of these features of online authentication will have a long-term impact on e-business.

The DC issued by a service provider can be categorized according to internationally recognized classes of certificates (Globalsign, Inc., 2002). This categorization depends on the confidence one may have in the identity given by the verification process. The growth in the number of applications of DS technology has resulted in the emergence of product and service differentiation. Some CA service providers focus on high value transactions such as finance, health care and government transactions, which require a very high level of security. Other firms provide strong support to network developers as well as Web server security. With the rapid development of m-commerce, the applications of DS are being extended to wireless solutions and m-commerce applications. Products and services can also differ in the product features and services realized by differences in the DS technology used.

DS vendors provide products necessary to manage the DC and public key infrastructure. These vendors develop "keys" and other technical infrastructure such as encryption software. 'Smartcard Solutions,' developed by RSA Securities, Inc., are equipped with many important features that specify the accountability of the user in electronic transactions, authenticate the user and secure the storage of important credentials (RSA Securities, Inc., 2002). Since the implementation of DS technology requires a highly secure environment, Internet security is also one of the emerging fields for DS technology. Some companies have focused on the niche market for the security measures required for the implementation of digital signatures. Every DS technology should be flexible enough to allow for modifications as business needs of an organization change. Another area in DS technology is the development of plug-ins or ad-ins to existing applications. Adobe systems and Microsoft are the leading companies in this area, developing ad-ins and plug-ins for their popular software.

3. Legal Issues

The Utah Digital Signature Act was the first attempt to provide a legal framework to the technical advances and business applications of DS technology. The Global and National Commerce Act, which went into effect on October 1, 2000, is another law intended to boost the application of encryption processes for electronic authentication. This law is about online authentication, but does not recommend the use of any DS technology in particular (Phair, 2001). Many e-business analysts perceive this Act as a first step to providing a trustworthy infrastructure for e-business (Lucas, 2000). Following the legal validation of the use of DS technology, there has been an emergence of products and services that provide secure online authentication using encryption techniques. Many business organizations prefer DS to other types of security technologies. The involvement of government in a PKI depends upon the extent of risk and liability a CA is willing to take. The involvement of a CA as a trusted third party in the use of a DS may reduce the risk of bilateral disputes. A CA is an organization that issues public-key pairs for its subscribers to use and issues digital certificates to the subscriber's trading partners attesting to the ownership of their public keys (Kuechler and Grupe, 2003). Under the guidelines of the pioneering Utah Digital Signature Act, a "closed loop PKI" is a system in which the government reduces the risk and potential liability of a CA by acting as the highest level of CA. According to some analysts, in an "open loop PKI," criminals may be able to extrapolate the technical information available with the public key and may succeed in working out the private key. Such criminals could commit widespread fraud and the relying parties may suffer huge losses. However, CAs using open loop PKI have been taking the necessary measures to limit the potential liability and fraud resulting from the misuse of DS. For

example, one such CA, Verisign, binds all its subscribers by the 'webwrap' agreement, which clarifies and limits the risk and the potential liability of Verisign (Verisign PKI, 2002).

The legal framework becomes more complicated when we consider the international applications of DS. This is an important consideration for many multinational companies. In many countries like Australia, Japan and countries in the European Union, the legal framework for the use of DS is still in the developing stage. Furthermore, considering the liability and risk, it is very complex to develop international standards for DS.

4. Methodology

In order to understand development trends in the application of DS technology, data were gathered from the Lexis-Nexis academic database, which is one of the premier sources of consolidated business and industry news reports. News reports related to product and application developments utilizing DS technology were gathered, mainly from the PR Newswire and Business Wire news agencies. Relevant news reports, associated with the US domestic market, were gathered from January 1, 2002 to May 20, 2002. In order to improve the validity of the data, we considered only those news reports that discussed product introduction and development associated with the use of DS technology. Even though these data are not extensive, and may under- or over-represent some DS applications, they are a relatively fair indicator of the number of application developments in the area of DS technology for the Internet security industry, over this five-month time period. The search generated 125 relevant records, which were then classified as either B2B, B2C, or B2G., according to the target customers and entities involved in the transactions.

These applications were further categorized along two dimensions: the sectors or industries for which the application was developed, and the purpose of the encryption and DS technology used in the application. From a preliminary analysis, it was found that certain applications of DS technology were developed to satisfy the security needs of the organization, and other applications were developed for the specific purpose of authentication, while others were developed for both purposes. Such a classification provides detailed information about the application development trends in DS technology in early 2002.

For the purpose of our analysis, we considered all types of software security solutions that use DS technology. Even though 'encryption' can be considered as a broader term in this context, all the applications discussed in this paper were those that used DS technology in one form or the other. A DS technology can be considered as the combination of an encryption process and some other types of technologies, depending upon the needs of an application, rather than encryption alone. This summarization of the data provided a basis for understanding industry-specific application development trends in e-business.

5. Application Development Trends

DS technology gradually developed as an application of encryption processes. The initial market demand for DS products was created by computer software and online businesses, which needed a better security infrastructure and robust authentication systems. During the mid to late nineties, the rapid emergence of e-commerce increased the need for secure and authentic online transactions. At first, legal developments, such as the 1994 Utah Digital Signature Act (Utah Department of Commerce, 1994), encouraged the application of this technology primarily in the B2B and B2G modes of e-business. Later on, rapid developments in e-commerce and online businesses boosted the use of DS technology in the B2C mode of business transaction.

Once the legal infrastructure and basic technologies were in place, several other industries such as banking, finance, health care and service industries also started using this technology for secure business processes. At the same time, the market has seen the emergence of more robust software solutions for security. In the following sections, transaction-specific (B2G, B2C, and B2B) applications of DS technology are analyzed.

5.1 B2G Mode of E-Business

In the B2G environment of e-business, the implementation of DS technology gives rise to unique issues. Our analysis found that government has been slow to adopt DS products. Because of the high liability associated with government transactions, most businesses are reluctant to use DS technology to process transactions with the government over the Internet. As shown in Table 1, the total number of applications differs significantly across the three modes of e-business, B2C, B2B, and B2G ($p < .0001$, Chi-squared test). Only 17% of all applications identified were categorized as belonging to the B2G mode.

However, recent trends show that government services are gradually accepting DS compliant products in order to cope with technological developments and to satisfy the growing need for security. Strong market demand from businesses and other government departments may also be another possible reason behind government adoption of DS technology. For example, the Social Security Administration has adopted 'Simple Sign', an online secure signature suite developed by DS Trust, which assists the Administration in filing wage reporting documents between

businesses and federal agencies (Snapp, 2002). While most of the recently developed B2G applications of DS technology have been primarily developed to facilitate the increased security of data, in many cases these applications also had the purpose of authentication.

Table 1 - Application Development Trends for Digital Signature (DS) Products

Industry	**Mode of e-business**								
	B2C			**B2B**			**B2G**		
	S	**A**	**C**	**S**	**A**	**C**	**S**	**A**	**C**
Banking	1		2	2	1	2			
Computer Software	2		2	22	1	7	2	1	
E-commerce				6	1	5			
Energy				2		1			
Health care	1		1	5	2	2	2	1	
M-commerce	1			3		2			
Telecommunications					2				
Services				8	2	2	5	1	6
Miscellaneous	1		1	9		5			
Defense								1	1
Education									1
Total	6	0	6	57	9	26	9	4	8
Grand Total	12 (10%)			92 (73%)			21 (17%)		

Note: DS Application products are categorized as S = Security, A = Authentication, and C = Combination of both. The numbers in the cells indicate the number of applications developed in that particular category.

Some DS applications developed for government services may be considered Government-to-Citizen (G2C) types of applications. Most of the applications developed in the B2G mode allow the direct and extensive involvement of citizens. Such G2C applications are used in various government services ranging from defense services to general government administration services. Recent trends show that governments are also using DS technology in various services such as energy, health care and education. Recently, the East Orange Police Department of New Jersey started using multi-application smart card solutions, developed by RSA Security Inc., for rapid and secure access to sensitive data (Fortier and Allen, 2002). Because of the rapid development of DS technology and the growing concern about security, some government departments are modifying their industry-specific regulations. To ensure the privacy and confidentiality of citizens' personal data, some US government agencies are enforcing new regulations on industry. Such modifications to regulations are either proposed or have been implemented in order to comply with the increasing security demands of citizens. For example, recently the US Drug Enforcement Administration proposed a new rule requiring pharmacists and physicians to authenticate themselves using electronic signatures, including biometrics (Langnau, 2002).

Other applications developed for the government do not have the direct involvement of citizens. Such applications are used for transactions between different departments of the government and for transactions between government departments and private businesses. Some DS applications are developed for secure operations associated with government employee privacy and authentication, such as facilitating government services for government employees. The analysis of recent trends shows that applications developed for the Government-to-Business (G2B) and Government-to-Government (G2G) mode are relatively few compared to applications developed for the G2C mode. In this analysis, however, it is important to consider the relative differences in the requirements for secure transactions in these different modes. It is possible that the government may be recognizing that the need for security and authentication in G2C types of transactions are more important than for other types of transactions. Another possibility could be that there are fewer transactions, or a greater need for standardization, in the G2G and G2B mode compared to the G2C mode.

5.2 B2C Mode of E-Business

The whole concept of DS technology is based on the development of secure online communication, which would ensure basic functions such as non-repudiation, security, authenticity and message integrity (American Bar Association, 2002). However, the applications of DS technology are not only restricted to secured online communication. DS technology has also been used in diversified functions such as secured access, authentication and confidentiality. Further from its originally intended purpose of 'secure Internet communication', DS technology

has been extended to secure standard and mobile phone communication. As Table 1 shows, only 10% of the applications identified in our sample belong to the B2C mode of e-business.

For B2C commerce, customers still prefer to use a traditional signature rather than a DS. This may be due to a lack of trust in the complex mathematical algorithm that is used for the encryption and security of online transactions (Shiralkar and Vijayaraman, 2002). Many companies like CRYPTOCARD, and Tovaris, Inc., are developing secure e-mail environments by encrypting e-mails. Such environments can certainly provide message integrity. But acceptance of such e-mail as a DS entirely depends on the trust of the customer in the business that is involved in a particular B2C transaction. The encryption process used in DS technology provides online security to confidential information such as credit card numbers and other personal details. Because of a lack of trust in Internet security, individuals may prefer to carry out only low levels of financial transactions online. Even for these transactions, privacy concerns discourage the use of DS technology. However, from a seller's point of view, these applications authenticate online transactions and thereby provide security to their online business.

One of the major impacts of privacy concern is on health care companies and hospitals. Such firms are not confident about keeping individual customers' health information records online and about providing online treatment, even to customers authenticated by DS. Rather than rely on a DS to ensure the authenticity of the person, these companies prefer to use 'biometrics' technology, which "relies on individual physiology or behavioral traits to identify and authenticate an individual" (Levin-Epstein, 2002). Recent product developments include secure software suites that provide Web-based delivery of prescriptions and laboratory results.

The banking industry is also rapidly adopting various DS technology products. Some of these DS technology products, such as Fleet Data Excel (SM) used by Fleet National Bank, specifically deal with online data reporting services (Farley, 2002). Such products facilitate secure transactions between business entities and individual customers. Many banks and finance companies are adopting secure online applications for faster and secure application processing. This process can be considered as a next step in the facilitation of secure e-banking. Recently, Las Vegas-based Community One Federal Credit Union started using the 'Receipt Manager' suite developed by Bluepoint Solutions for reducing the expenses of having an 'off-site' storage location (Drew, 2002). Similarly, Arizona Central Credit Union started using an e-signature based transaction system developed by Interlink Electronics and Bluepoint Solutions (Roberts, 2002).

Other major DS technology product developments have been in the field of m-commerce. Secure e-mail products and m-commerce applications have been developed for use by individual consumers. Such products are mainly used for either Consumer-to-Consumer (C2C) or Consumer-to-Business (C2B) types of transactions. For example, the secure e-mail environment developed by CRYPTOCARD ensures message integrity and message privacy for consumers (Keeffe, 2002). Similarly, the electronic wallet for mobile services developed by CIC can be used as a signature wallet for a personal digital assistant (PDA), ensuring the confidentiality of personal data (Eshghipour, 2002). Such integration of various technologies in PDAs and cell phones has expanded the scope of applications for DS technology and encryption.

From the market trends observed in our sample, it may be concluded that relatively very few applications have been developed for the B2C mode of transactions. However, the rapid development of the B2C mode of e-business and the further deployment of online and mobile communications will certainly promote the technological development of new DS products for the B2C mode of e-business.

5.3 B2B Mode of E-Business

Most B2B transactions involve a high dollar value and a higher level of financial risk and accountability, compared to B2C transactions. Many companies have developed different DS technology products that satisfy the security as well as the business needs of different types of businesses. Such products aim to accelerate business processes and improve business efficiency. As shown in Table 1, our study shows that 73% of the applications identified in our sample belong to the B2B mode of e-business. Applications of DS technology in the B2B mode have been implemented in almost all types of industries.

Technological development, and government support in the form of legislation, has boosted the use of DS technology in the B2B mode of e-business in recent years. Despite different 'claims' of 'highest online security' provided by competing products, many businesses are still reluctant to trust DS technology (Karpinski, 2000). Instead of using DS technology for signing business contracts online, companies are using it as a means of authenticating and validating online information. Encryption technology is being used in many B2B applications such as smart-card solutions, Secure Socket Layer (SSL), and other online authentication applications, mainly because it provides security and non-repudiation of the data.

Recent market trends show that there is a considerable increase in the use of DS technology in the banking and finance sectors (Table 1). These applications range from encryption pin pads developed by Diebold to an e-pad handwritten electronic signature solution developed by Interlink Electronics. In some cases, the applications have

been developed for the purpose of securely integrating existing systems. Generally, businesses outsource their system security requirements to software vendors. These software vendors develop scalable DS compliant products and integrate them with existing systems. Such products are developed mainly to serve the security needs of the current systems. Considering this application area for DS technology products, recently the computer software industry witnessed several collaborations and strategic partnerships for the development of better and more secure DS technology solutions. For example, a technology partnership between Unisecurity, Inc. and Netgrity was formed to integrate the SecuForce ™ suite of Unisecurity, Inc. with the Siteminder® Platform of Netgrity (UniSecurity Inc., 2002).

Other major DS technology applications were found in the health care industry. The applications range from health care authentication systems to online authentication of medical records. Again, some of these applications are developed through strategic alliances. For example, MedUnite, Inc. integrated its transaction platform with the health care authentication system of Verisign, Inc., which enabled secure online communication for physicians (Blevins, 2002). Industries in the services sector are also one of the major application areas of DS technology. These services mainly include, but are not limited to, retail businesses. These applications include secure payment terminals and signature-capture terminals, to name a few.

Compared to other modes of e-business, the B2B mode has a relatively higher number of online transactions. Correspondingly, the B2B mode has a relatively higher demand for online security applications. The market has responded to this demand with a number of developments in DS technology. This can be observed from the comparative analysis (Table 1) of technological developments in DS technology across all three modes of e-business.

6. Conclusion and Implications for Businesses

In order to understand the use of DS technology in the future, it is important to study trends in the use of various DS technologies. From our data, we found that most of these technologies fall under the categories of biometrics, secure data transactions, secure e-messaging, wireless security, secure data access, and other tailor-made or standardized technologies. Industry trends show that in most of the cases, secure e-business suites utilize combinations of various technologies. Such solutions possess a high level of scalability and customizability. As shown in Table 2, in our sample these solutions constituted 62.4% of the total number of applications developed. Further, most of these applications were developed for the B2B mode of e-business. However, there are many other applications that utilize certain specific DS technology. For example, e-messaging technologies and secure data access technologies each constituted 10.4 % of the total number of applications developed (Table 2). Secure wireless technologies (5.6%) were yet to gather this pace of development. The distribution of DS technologies differed significantly across e-business modes (p = .003, Chi-squared test). For example, e-messaging and data security constituted the majority of solutions developed for the B2C mode of e-business, whereas the greatest number of applications developed for the B2G and B2B modes were tailor-made DS technologies.

Even if the majority of the present application developments in DS technology are in the B2B mode, B2C applications are likely to grow with a faster pace in the future. The rapid development of DS technology applications for m-commerce, health care, and banking imply potential growth opportunities in the B2C mode of e-business. Another major impact of DS products on the B2C mode of e-business may be realized in terms of increasing perceptions of trust in secure online business transactions. In the B2C mode of e-business, consumers perceive the term 'Thawte Certified' or the appearance of a Verisign logo on a Web site as a symbol of trust and security. This change in consumers' perceptions of online transactions will improve e-business in the long-term.

We found that application developments in DS technology responded more to certain sectors of the economy compared to other sectors. The primary reason behind this may be varied needs for secure business processes in different industries. For example, a security breach in the health care industry poses different issues and risks compared to a security breach in the banking and financial services industries. In the same way, the security needs of a government defense department are different from the security needs of the wireless infrastructure for m-commerce.

Irrespective of the type of e-business, we found that the purpose of most applications of DS technologies is to secure business transactions and processes. In our sample, seventy-two applications (58%) dealt exclusively with the security of transactions, whereas forty applications (32%) were intended to solve the problem of security as well as authentication. Only thirteen applications (10%) were developed mainly to ensure the authenticity of entities involved in transactions.

Depending upon these varied needs across industries, the market responds to the demand by developing solutions to build a robust and secure online infrastructure. The availability of secure infrastructure will promote e-business further among many brick and mortar companies. These developments will certainly lead to necessary

modifications in the existing legal infrastructure. Further developments in DS applications and the legal infrastructure in the international arena can increase the efficiency of global businesses.

TABLE 2- Trends in Use of Various Digital Signature Technologies

Digital Signature Technology	**Mode of Business**			**Total Applications developed**
	B2G	**B2C**	**B2B**	
Biometrics technology	2	1	2	5 (4.0%)
Secured data transaction technologies	2	2	5	9 (7.2%)
Secured data scanning and data access technologies	3	3	7	13 (10.4%)
Secure electronic messaging	3	4	6	13 (10.4%)
Wireless security and authentication	1	3	3	7 (5.6%)
Other tailor-made DS technologies	12	1	65	78 (62.4%)

Note: Other tailor-made DS technologies refer to combinations of the other technologies mentioned above. For example, a secure e-business suite can utilize secure data electronic messaging such as Secure Socket Layer (SSL), secure data access, as well as secure data transactions.

Among the DS technology products recently introduced to the market, businesses can choose from many security options that provide the 'same' basic functions of security, authentication, and non-repudiation. Apart from standardization, it is important to have reliable evaluation techniques to compare the quality of different DS technology products. Even if businesses have some sort of 'trust' in claims of 'unbreakable codes' embedded in DS technology products, there has been very little research done on the qualitative evaluation of DS products as a whole. Further research in this area will assist the vendors of DS products to provide better and more qualitatively reliable security solutions, which in turn will further boost e-business.

REFERENCES

American Bar Association, "Digital Signature Guidelines Tutorial," Section of Science and Technology Information Security Committee, 2002, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html, Last accessed on September 20, 2002.

Blevins, J., "Medunite To Adopt Verisign Authentication Technology To Safeguard Electronic Patient Records; AMA Internet ID to Verify Physician Identities for Secure Medunite Transactions," PR Newswire, January 30, 2002.

Drew D., "Community One Federal Credit Union Goes Paperless," Business Wire News, January 21, 2002.

Eshghipour C., "CIC Releases First Electronic Wallet for Mobile Devices With Biometric Protection," PR Newswire, May 16, 2002.

Farley, S., "Fleet Introduces Online Data Reporting Service for Government Clients," Business Wire, May 16, 2002.

Fortier, R. and R. Allen, "New Jersey Police Department Selects RSA Security to Help Take A Bite Out Of Crime; East Orange Police Department Using RSA Security to Help Lock Down the Department's Crime Reports, Arrest Files and Criminal Records," PR Newswire, February 25, 2002

Gelboard, B., "Signing Your 011001010: The Problems of Digital Signature," *Communications of the ACM*, Vol. 43, No. 12:27-28, December 2000.

Globalsign, Inc., Home page of Globalsign, Inc., 2002, http://www.globalsign.com, Last accessed on August 16, 2002.

IDCertify, Inc., Home page of IDCertify, Inc., 2002, http://www.idcertify.com, Last accessed on August 16, 2002.

Karpinski R., "Who can you Trust?," *B to B*, Vol.85, No. 11:1, July 31, 2000.

Keeffe, M., "CRYPTOCARD Smart Card Supports Microsoft; CRYPTOCARD's SC-1 Smart Card Enables Microsoft Users to Digitally Prove Identity", Business Wire, May 1, 2002.

Kuechler, W. and F. Grupe, "Digital Signatures: A Business View," *Information Systems Management*, Vol. 20, No. 1:19-28, Winter 2003.

Langnau, L., "The FDA's data mandates—and why you should care," *Material Handling Management*, Vol. 57, No. 7:37-44, July 2002.

Levin-Epstein M., "Dealing With Security", *IT Health Care Strategist*, Vol. 4, No. 4:1-6, April 2002.

Lucas, P., "Congress Signs Off On Digital Signatures," *Credit Card Management*, Vol. 13, No. 7:29-34, October 2000.

Phair, M., "New Laws, Technologies Push Signing On The Dotted Screen," *ENR*, Vol. 246, No. 8:47-50, February 26, 2001.

RSA Securities, Inc., Home page of RSA Securities, Inc., 2002, http://www.rsa.com, Last accessed on August 16, 2002.

Roberts, K., "Interlink Electronics And Bluepoint Solutions Announce E-Signature–Based Transaction System; Arizona Central Credit Union First Customer To Deploy," Business Wire News, Jan. 16, 2002.

Shiralkar, P. and B.S. Vijayaraman, "Impact of Digital Signature Technology on E-business," *Proceedings of the National Meeting of Decision Sciences Institute*, San Diego, CA, November 2002.

Snapp, C., "Digital Signature Trust Introduces Simplesign ™, Easy-To-Use Digital Document Signing Application; Social Security Administration to Use Simplesign For Signing And Filing Wage Reporting Documents Between Businesses And Federal Agencies," PR Newswire, January 7, 2002.

UniSecurity Inc., "Unisecurity Partners With Netegrity To Provide The Missing Link To Complete End-To-End Sign-On SSO- Solution for SAP", Business Wire, May 6, 2002.

Utah Department of Commerce, Division of Corporation and Commercial Code, "Utah Digital Signature Act", 1994, http://www.le.state.ut.us/~code/title46/46_03.htm, Last accessed on September 20, 2002.

Verisign, Inc., Home page of Verisign, Inc., 2002, http://www.verisign.com, Last accessed on August 16, 2002.

Verisign PKI, "Public–Key Infrastructure (PKI)—The Verisign Difference," 2002, http://www.verisign.com/whitepaper/enterprise/difference/difference.html, Last accessed on February 10, 2002.

Wright, B. "Technology file: La ws guide uniformity for e-signatures", *Credit Union Executive Journal*, Vol. 40, No. 12:17, Nov./ Dec. 2000.