A Web-Centric Framework for Secure and Binding Electronic Transactions

By

Kiran K Choudary

Bachelor of Technology (Honors), Indian Institute of Technology, Kharagpur, India

Submitted to the Department of Civil and Environmental Engineering in partial fulfillment of the requirements for the degree of

Master of Science

at the

Massachusetts Institute of Technology

May 18th, 2000

[June 2000]

Author.....

Department of Civil and Environmental Engineering

/ May 18th 2000

Certified By.....

Feniosky Peña-Mora

Associate Professor of Civil and Environmental Engineering

rvisor

Accepted By.....

Daniele Veneziano

Chairman, Departmental Committee on Graduate Studies

A Web-Centric Framework For Secure and Binding Electronic Transactions

by Kiran K Choudary

submitted to the Department of Civil and Environmental Engineering on May 18th, 2000
in partial fulfillment of the requirements for the Degree of Master of Science

Abstract

The goal of this thesis is to present a web-centric framework for conducting secure and legally binding electronic transactions. This framework would create the confidence to achieve a large-scale replacement of paper-based transactions prevalent today, with secure and legally binding electronic transactions. The approach used - in this research effort - in achieving this goal, is two-phased. While the first phase focuses on developing a framework for conducting secure and legally binding transactions in a specific industry namely, the $3.2 Trillion construction industry, the latter part of the thesis addresses the security needs of e-commerce transactions in general through the development of an e-Notary service. The A/E/C specific implementation, in the first phase of this research effort not only provides very valuable insight into some of the most important concerns in conducting electronic transactions today, but also highlights the technology components required to conduct secure and legally binding transactions over the Internet, through the creation of models for secure communication and secure information management. Thus, it serves as a precursor to create a generic framework for conducting secure electronic transactions through the development of an e-Notary service, in the second phase, that provide secure and legally binding third-party security services to transaction service providers like e-commerce corporations and government organizations, enabling these organizations to focus on their core business.

Thesis supervisor:

Feniosky Peña-Mora, Associate Professor of Civil and Environmental Engineering

Acknowledgements

I would like to thank my thesis and research advisor Professor Feniosky Peña-Mora for his invaluable support and guidance during this research effort. I would like to thank him for funding my education at MIT through a research assistantship over the last two years, as well as, for advising me on my career decisions.

I would also like to thank the Central/Artery Tunnel Project, Boston and Penop Inc., New York for their financial support, in the form of research grants that supported my research assistantship at MIT.

Our research group, the DaVinci Research Society, has been a great resource during the last two years and I would like to particularly thank my friends Sanjeev Vadhavkar, Paddu Vedam, Jaime Solari, Justin Mills, Chang Kuang, Gyanesh Dwivedi, Ajit Sutar, Sugata Sen, and Tong Li for the fun-filled days I have had, within and outside MIT. I would also like to thank my other IESL lab mates - apart from the DaVinci members - Jayaprakash Pasala, Petros Komodromos, Abel Sanchez, and Emma Shephardson for the wonderful time I have had at IESL.

Finally, I would like to thank Joan Mckusker (Joanie) and Cynthia Stewart for all the help I took from them over the last two years that I have been here at MIT.

" This thesis is dedicated to my family - my parents and my sister – who have always supported and motivated me towards achieving my goals."

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Day-to-day business operations in corporations, engineering projects and the government involve collaboration between a number of organizations. These organizations conduct business with one another by participating in a large number of business-to-business (B2B) transactions, through which they not only allocate resources and funds but also transfer responsibilities and risk between one another, over a period of time. The legal nature of these transactions makes the participants accountable for the agreements/commitments made on them. Currently, most of these transactions are not conducted electronically. They are conducted in the form of paper-based documents – 90% of all forms are paper [Forms Institute, 2000] - which are approved by the representatives of organizations participating in these transactions.

The importance of IT has been increasing exponentially during the last decade - it is viewed as a core competency that would help raise productivity, profitability, and service quality and hence increase competitiveness in the global marketplace. With the emergence of the Internet and vast improvement in communications/networking technologies in the last few years, there is ample potential to build a web-based framework to electronically conduct transactions between geographically distributed transaction participants. Since the electronic transactions would also involve commitments that make the participants legally accountable, they need to be at the least as secure and tamper-proof as their paper-based counterparts. The focus of this thesis is the development of a framework that would facilitate secure and legally binding electronic transactions between distributed transaction participants. This framework would create the much-needed confidence in industry, government, as well as, the consumer to achieve a major replacement of paper-based transactions with secure and legally binding electronic transactions.

1.2 Objective

The goal of this thesis is to develop a web-centric framework, including a working prototype, for conducting secure and legally binding electronic transactions. The thesis aims to address issues of conducting secure and legally binding transactions across different kinds of e-commerce transactions namely, business-to-business (B2B), business-to-government (B2G), business-to-consumer (B2C) and government-to-consumer (G2C). Another one of the objectives of the research effort was to incorporate a wide range of security technologies – biometrics, infometrics and public key infrastructure (PKI) – into the framework, which would also serve to provide reliability (through redundancy) and scalability in the architecture. Apart from developing the framework, the thesis also aims to study technology-related, as well as, organizational issues related to deploying this framework in large organizations.

1.3 Methodology

The methodology followed in addressing this research problem can be broadly divided into two phases. During the first phase, this research effort focused on developing a framework for conducting secure and legally binding business-to-business (B2B) transactions within a specific industry, namely the $3.2 trillion A/E/C industry [Bidcom, 2000]. The A/E/C industry, because of its structure and organization, size, geographically distributed nature and reluctance to achieve large-scale replacement of paper-based transactions, proved to be a perfect test-bed for developing the framework and achieving a major transition to electronic transactions. The initial period, of this phase, was used to study the security concerns of conducting electronic transactions in large-scale A/E/C projects. These concerns, to a large extent, proved to be similar to security concerns in other industries, in conducting electronic transactions, and hence the framework developed for large-scale A/E/C projects could be extended across industry segments. This phase was also used to identify and study the security technologies that are needed to be incorporated into the framework for achieving secure and legally binding electronic transactions. It also served to provide feedback on technology- related, as well as, organizational issues related to large-scale, IT driven, business process re-engineering.

The second phase of this research effort addresses the generic problem of conducting secure and legally binding electronic transactions over the Internet, through the development of an e-Notary service that would provide security services to web-based transaction service providers, like e-commerce corporations. The A/E/C implementation - during the first phase - provided both, a set of requirements, as well as, technology solutions that were used in the development of the e-Notary service. The e-Notary service fulfills the objective of conducting secure and legally binding transactions across business-to-business (B2B), business-to government (B2G), business-to-consumer (B2C) and government-to-consumer (G2C) e-commerce transactions.

1.4 Thesis Organization

As explained earlier, the research effort, on which this thesis is based, is two-phased. The first part of the thesis (Chapters 2-7) focuses on business-to-business (B2B) transactions within a specific industry, namely the $3.2 Trillion A/E/C industry. It addresses the security concerns in conducting legally binding electronic transactions in large-scale A/E/C projects by developing a framework for conducting secure and binding electronic transactions in large-scale A/E/C projects. After defining the stringent requirements of a framework that satisfies the security concerns in conducting electronic transactions in large-scale A/E/C projects in Chapter 3, the inadequacy of the available web-based project management systems in meeting these requirements is studied in Chapter 4. This is followed by a discussion on the two main issues involved in the development of the framework, namely, secure communication in Chapter 5 and secure information management in Chapter 6. Finally in Chapter 7, issues related to the implementation of the proposed framework at the decade-long $13.6 billion Central Artery/ Third Harbor Tunnel Project in Boston, USA are discussed.

Following the development of a framework for conducting secure and legally binding electronic transactions for a specific industry segment namely, large-scale A/E/C projects, the latter part of the thesis consists of the development of a generic framework for conducting secure and legally binding transactions between businesses, the government and consumers. The framework consists of an e-Notary Service that would provide security services to web-based transaction service providers, like e-commerce corporations, for conducting secure and legally binding electronic transactions, while the organizations themselves focus on their core business. Chapter 8 motivates the need for a generic framework for conducting secure and legally binding electronic transactions, based on the research conducted in the first phase of the thesis. While Chapter 9 introduces the vision of an e-Notary service and discusses its functional architecture, Chapter 10 discusses the implementation of a prototype version of an e-Notary service, including the system architecture, its components and application on a test case, namely a web-based stockbroker.

Having developed a framework for secure and legally binding business-to-business transactions, specifically in large-scale A/E/C projects (Chapters 2-7), followed by a generic framework for secure and legally binding electronic transactions between businesses, the government and consumers, Chapter 11 concludes this thesis by summarizing the thesis, and the results and benefits of this research effort followed by a discussion on the scope for future research.

Chapter 2

A Framework for Conducting Secure and Binding Electronic Transactions in Large Scale A/E/C Projects

2.1 Background

The importance of information technology (IT) in the $3.2 Trillion construction industry has been increasing in recent years [Bidcom, 2000]. IT is now being viewed as a possible core competency that would help engineering corporations increase productivity and profitability, making them more competitive in the global market. Currently, a large part of the planned IT investments made in large scale engineering projects, is in the design stages of the project - in the form of CAD systems (hardware and software), simulation and modeling packages – and in project monitoring and control during the construction phase. Unlike other industries, integrated management information systems have, till recently, been a low priority as far as IT investments in large scale engineering projects are concerned. Now, senior management at large engineering corporations have realized

the important role information technology has often played in increasing service quality and productivity in other industries like manufacturing, financial markets, transportation and logistics. This realization that the use of IT for large-scale project management can increase efficiency and productivity considerably, is motivating large-scale A/E/C projects to strive towards automating their project management processes.

An integral component in the management of large-scale engineering projects is the management of business-to-business (B2B) transactions between organizations participating in the projects. These organizations are typically involved in a large number of transactions through which resources in the form of people, materials and funds are allocated, over a period of time. Transactions are also conducted for day-to-day issues like assigning an architect the responsibility of a design analysis report, shifting of a deadline or requesting an increase on the contractor budget. The very nature of these transactions, make their participants legally accountable for the commitments made in them. Hence, there is a need for conducting them in a manner that is secure and binding, making it acceptable to the participants of the transaction.

Currently, most of these transactions are not conducted electronically. They are primarily conducted in the form of paper-based contractual agreements, which are approved by the representatives of the participating organizations using handwritten signatures, sealed, distributed using courier/postal services and finally physically filed and stored in cabinets. These paper documents (both in original form and copies) are used to resolve any dispute that may arise between the organizations that were involved in the contract. In the case of a legal claim or settlement, the signatures - of the approvers - on the documents are used to legally uphold the commitments made in them, by the organizations represented by the signatories.

2.2 The Need for a framework for Secure and Binding Electronic Transactions

Advancements in Information Technology and the growth of the Internet has generated a host of web-based project management services (external to the project) to automate

transaction management in the $3.2 Trillion construction industry [Bidcom, 2000], which till now has largely been ignored or under served by high-tech software application developers who have not recognized the distinct needs, or realized the vast potential, of this business. Though, these services automate transaction management, they are inadequate in satisfying some of the stringent security requirements for conducting secure and legally binding electronic transactions in large-scale A/E/C projects. This inadequacy has prevented the creation of confidence in the construction industry to view these services as a viable alternative to paper-based transactions. Thus, though a section of the A/E/C industry is availing these online project management services, most large-scale A/E/C projects still conduct paper-based transactions in parallel, and do not conduct some of their more critical transactions online. Nevertheless, the currently available online services have generated considerable interest in the A/E/C industry, which is looking forward to the next generation of online project management services/ products that satisfy their stringent security needs and give them the confidence to replace (to a large extent) paper-based transactions, with secure and legally binding electronic transactions.

Thus, there is a need to utilize the vast improvement in communication and security technologies in the last few years to build a web-centric framework to conduct secure and legally binding electronic transactions. This framework would allow secure and legally binding electronic transactions, between the geographically distributed organizations in large-scale A/E/C projects, enabling the construction industry to achieve a major replacement of paper-based transactions. Since the electronic transactions in large-scale A/E/C projects would also involve commitments that make the participants legally accountable, they need to be at the least, as secure, binding and tamper-proof, as their paper-based counterparts. Thus, a framework for secure electronic transactions should at least offer the same level of security and legal acceptability as the paper contracts offer in the non-electronic environment.

2.3 Summary

In the following five chapters (Chapters 3-7), a framework for conducting secure and binding electronic transactions between organizations (see Figure 2 –1) participating in a large-scale A/E/C project is presented.

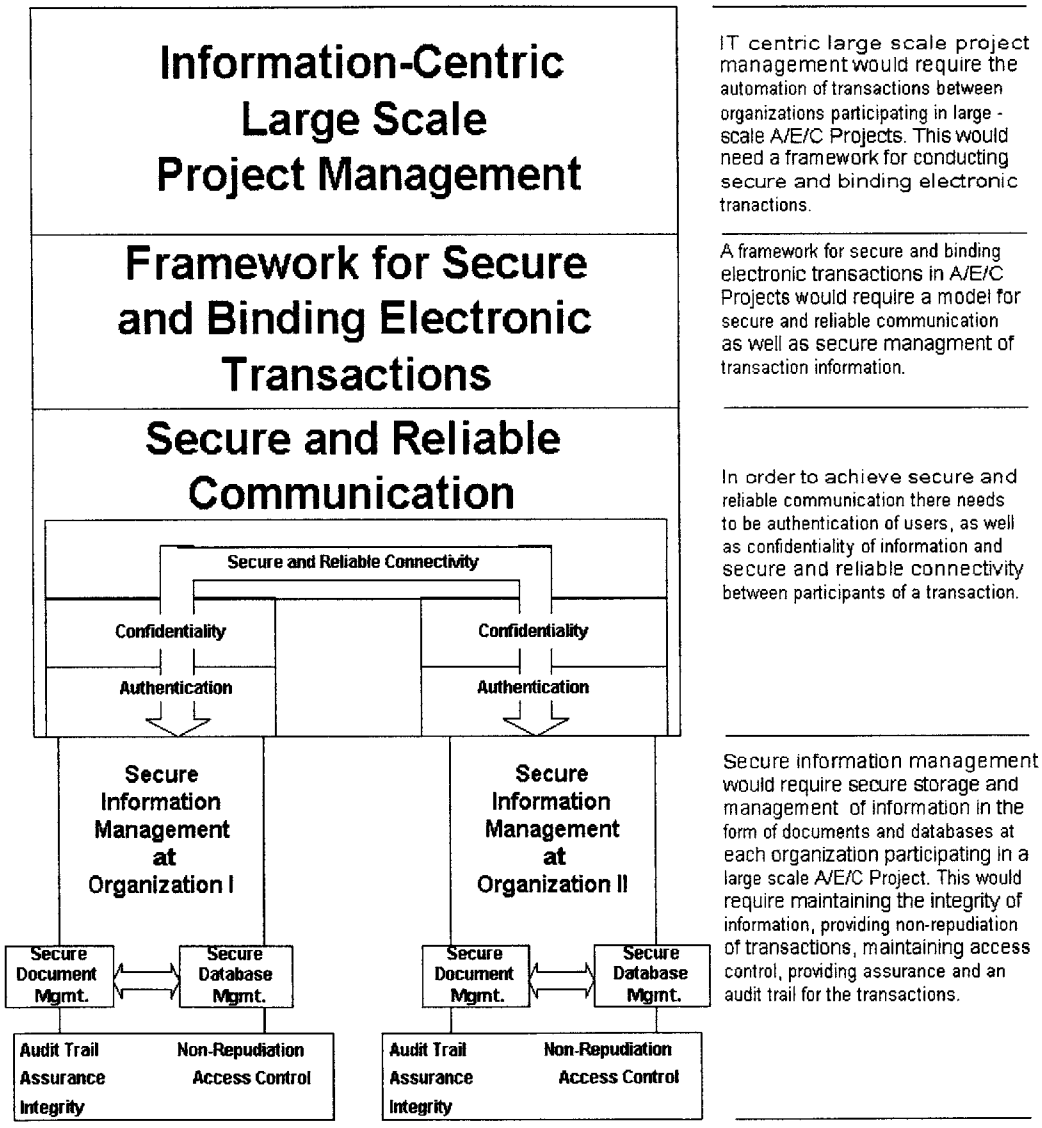


Figure 2-1: Framework for Secure Electronic Transactions in Large-Scale AEC Projects

In order to present a framework for conducting secure and legally binding electronic transactions, the security needs for a large-scale A/E/C project must first be ascertained.

In the following chapter, the security requirements for conducting legally binding electronic transactions in large-scale A/E/C projects are defined. This is followed, in Chapter 4, by a review of existing web-based project management services in light of the security requirements for electronic transactions in large-sale A/E/C projects, as defined in Chapter 3. The framework itself will be presented within a two-pronged approach. Firstly, in Chapter 5, a model for secure and reliable communication is presented. This model focuses on the secure and reliable flow of information between the participants of a transaction through the integration of technologies like digital IDs for identification, non-repudiation and confidentiality, and virtual private networks for secure and reliable connectivity and reasonable Quality of Service (QOS). Secondly, in Chapter 6, a model for secure management of transaction information is introduced. This model focuses on the secure storage, retrieval and management of transaction information, in the form of electronic documents and databases, by integrating technologies like integrity checking algorithms, biometrics and digitized signatures, for maintaining the integrity of transaction information, as well as, providing non-repudiation, an audit trail and controlling access to transaction information. A case study of the use of the framework, and the issues related to deploying the framework, developed in this thesis, is presented in Chapter 7.

Chapter 3

Security Concerns for Electronic Transactions in the A/E/C Industry

As a first step in presenting a framework for conducting secure and binding electronic transactions in large-scale A/E/C projects (see Figure 2-1), the security requirements for conducting electronic transactions in large-scale A/E/C projects, must be ascertained. The requirements presented in this section were identified as a result of interviews with A/E/C project personnel, as well as, reviews of transactions conducted in large-scale A/E/C projects.

3.1 Identification and Non-Repudiation

Due to the presence of a large number of participating organizations and individuals, there is a need to ensure complete transparency by precisely identifying each transaction participant, and legally binding him/her to the transaction. In paper-based transactions, the seal of the organization and the hand-written signatures of the organizations'

representatives identify the transaction participants. The seals and signatures on paper documents not only provide a good trace of the parties sending the document, but also, prevent the transaction participants from denying their participation in the transaction, thus legally binding them to the transaction. Thus, the identification mechanisms, to be used in any legally binding electronic transactions, should be such that they are extremely difficult to forge or misuse, and hence non-repudiate. At the same time, the identification scheme should be scalable to paper-based documents too, i.e. if paper-copies are made (from electronic data) after the transaction, the paper-copies, on their own, should precisely identify transaction participants and provide non-repudiation, in a legally binding fashion.

3.2 Confidentiality

Since transaction information would travel across organizational boundaries it needs to be secured from unauthorized viewing (within, as well as, outside an organization). In paper-based transactions the contractual documents are typically sent in sealed envelopes hidden from the public view. Similarly, in electronic transactions there is a need to protect the transaction information, which would contain confidential information relating to contracts, from unauthorized viewers. Confidentiality of information needs to be maintained not only during transmission of information i.e. during the transaction, but also, after the transaction has been conducted, just as paper-based contracts are securely filed in cabinets.

3.3 Integrity

Transaction information is vital in the case of legal disputes and claims during and after the project [CA/T Project, 2000]; it needs to be secure from intentional and unintentional tampering. In paper-based transactions copies of contractual documents are sent from one organization to another securely after being sealed in envelopes, and are then securely filed and stored by all the organizations participating in the transactions. Existence of multiple copies (with the original paper copy usually being sent to the recipient of the

transaction information) of the paper documents (at least one with each organization) prevents a particular organization from tampering or modifying transaction information to their benefit. In the electronic transactions scenario there is a similar need to secure transaction information from being tampered during or after a transaction. Transaction related information in A/E/C projects is typically stored in electronic documents from which information is extracted to database management systems for better organization of data, and faster search and retrieval. Hence the integrity of transaction data in each of these data repositories needs to be also maintained.

3.4 Access Control

Paper-based contracts are securely filed in cabinets under lock and key and only authorized personnel can access the contractual documents. Similarly, in electronic transactions, transaction management systems (and the underlying transaction data in databases and documents) have to be secured against unauthorized access. Access control is needed, not only to prevent unauthorized users to view (and, potentially change) transaction data, but also to prevent users to view data for specific kinds of transactions, say a Change Order, for which they do not have authorization. While the first step in providing access control is precisely identifying the users (see Identification and Non-Repudiation, discussed earlier in this section), once this is done the users' level of authorization would also have to verified based on his/her credentials like designation, department.

3.5 Assurance

In paper-based documents, a broken seal on an envelope might indicate that someone had read (without authorization) or tampered with a document. In electronic transactions too, there is a need to provide a similar mechanism to the participants of the transaction, which would assure them about the integrity of the transaction information, both during the transmission of data, as well as, after the transmission of data. For example, a project

representative should know that a document had been modified after he/she approved it, if it happens.

3.6 Audit Trail

An audit trail is needed to provide the organizations participating in a large-scale A/E/C with evidence about the actions of transaction participants. For instance, it would provide information like the reason for a particular transaction being approved by a particular project representative. The audit trail should provide digital evidence that has legal weight in order to uphold the validity of transactions during claims, after the completion of the project.

3.7 Reliability of transaction infrastructure

Large-scale A/E/C projects typically have a large number of transactions and the execution of these transactions in a timely and efficient fashion is vital to the functioning of projects. Paper-based transaction management maybe time-consuming, but nevertheless it is a reliable mechanism to conduct transactions. Hence, the electronic transaction infrastructure should offer the same reliability as in the case of their paper-based counterparts. The infrastructure should possess ample redundancy and Quality of Service (QOS) in its architecture to minimize the occurrence of delay or failure, which would be unacceptable in this critical application.

3.8 Scalability

The large investments, in time and funds, in building an electronic transaction infrastructure can only be justified if it possesses a fair degree of scalability allowing it not only to be, ported to different kinds of projects with ease, but also to be compatible with technologies of the future. At the same time, some components of the framework should be compatible with paper-based transactions, which is currently the primary mode for conducting transactions in large-scale A/E/C projects, and will be in use in the future,

albeit to a lesser extent. For example, as discussed earlier in this section, the identification scheme for transaction participants should be such that if paper-copies are made after the transaction they should precisely identify transaction participants and provide non-repudiation, in a legally binding fashion.

3.9 Summary

This chapter discussed the security concerns that serve as the requirements for developing a framework for conducting electronic transactions in large-scale A/E/C projects. Prior to developing the framework for secure and binding electronic transactions, a review was conducted to estimate the extent to which web-based project management systems, currently available for use in A/E/C industry, satisfy the requirements for secure and binding transactions in large scale A/E/C Projects, as defined in this chapter.

Chapter 4

Existing Web-based Project Management Systems: A Security Review

The advent of the Internet has ushered in a host of web-based project management services, as well as products, to serve the A/E/C industry. While most of these offerings provide for electronic transactions between organizations participating in large-scale A/E/C projects, there has been less focus on making these transactions sufficiently secure (effectively addressing all the security concerns identified in Chapter 3) and legally binding, hence having to rely on mutual trust between parties, as well as, paper-based transactions in parallel. In order to evaluate the adequacy of the currently available project management services in providing secure and legally binding transactions for large-scale A/E/C projects, some of the most popular services [see Table 4-1] were reviewed, in light of the requirements defined in Chapter 3.

4.1 Identification and Non-Repudiation

The web-based project management systems that were reviewed (see Table 4-1) rely primarily on password-based identification of users. Passwords are not only easy to steal and misuse [Privacy Exchange, 2000], but are also inconvenient to use since they need to be regularly changed (to ensure a minimum level of security) making it tough to remember them, especially if the users have multiple passwords. Identification through passwords does not provide non-repudiation (since it is easy to claim that one's password had been stolen and misused) hence the transactions where users identify themselves through passwords could be legally challenged in most cases [Privacy Exchange, 2000]. Transaction participants need to be identified by a unique human trait that is extremely difficult to forge (and hence misuse) or by a mechanism where a trusted third party provides authentication.

4.2 Confidentiality

Confidentiality of transaction information is provided by Secure Socket Layer (SSL), which provides for encryption of all data that is transmitted. SSL was created by Netscape Corporation (Netscape Corporation, 2000) to provide secure communication over TCP/IP based networks. Though the SSL specification (Freier, Karlton, Koshers 1996) provides for server authentication to client, client authentication to server, encryption of communication and integrity of data transmitted, it has been implemented in various ways by e-commerce services. The SSL implementation in the project management systems that were reviewed, provides encryption and integrity of transaction data during transmission, but lacks authentication between client and server, that is crucial for identification and non-repudiation.

4.3 Integrity

Integrity of transaction data is secured during transmission using SSL but the integrity of data after transmission is secured using access-control mechanisms (that prevent users

from modifying data through their accounts once transactions have been committed). This technique is insecure since it leaves open the possibility that data may be tampered accidentally by system administrators (say, during backup or porting across platforms), or intentionally by hackers since the access-control is based on password-based identification of users.

TABLE 4-1: A Review of Security in Existing Web-based Project Management Systems

	Identification	Non-Repudiation	Confidentiality	Integrity of Transaction Information	Access Control	Assurance	Audit Trail	Reliability	Scalability
Active Project	Password	×	×[1]	×[1]	Yes, but use a Password ID	None against Integrity	√[2]	Internet dependent	√[3]
BuildPoint	Password	×	Encrypted during transmission	Maintained during transmission	Yes, but use a Password ID	None against Integrity[4]	√[2]	Internet dependent	√[3]
BuzzSaw	Password	×	Encrypted during transmission	Maintained during transmission	Yes, but use a Password ID	None against Integrity[4]	√[2]	Internet dependent	√[3]
ProjectNet	Password	×	Encrypted during transmission	Maintained during transmission	Yes, but use a Password ID	None against Integrity[4]	√[2]	Internet dependent	√[3]
Insite	Password	×	×	×	Yes, but use a Password ID	None against Integrity	√[2]	Internet dependent	√[3]
Project Grid	Password	×	Encrypted during transmission	Maintained during transmission	Yes, but use a Password ID	None against Integrity[4]	√[2]	Internet dependent	√[3]
Prolog Website	Password	×	×[1]	×[1]	Yes, but use a Password ID	None against Integrity	√[2]	Internet dependent	√[3]
Project Wise	Password	×	×[1]	×[1]	Yes, but use a Password ID	None against Integrity	√[2]	Internet dependent	√[3]
Proposed Framework	Digital Certificates, Digitized Signatures and other Biometric IDs	√	Encrypted during transmission	Maintained during transmission and after transaction	Yes, and use Digital Certificates, Digitized Signatures and other Biometric IDs for identification	√	√	VPN Service Dependent	√

[1] Does not use SSL by default, but SSL support can be added by projects deploying this product
[2] No audit trail evidence for approval of documents
[3] Limited scalability to paper-based transactions
[4] Post-transaction integrity

Source: Active Project [Framework Tech, 2000], BuildPoint [BuildPoint Corp, 2000], Buzzsaw [Buzzsaw.com Inc, 2000], ProjectNet [Cephren Inc, 2000], Insite [Bidcom 2000], Project Grid [RII, 2000], ProjectWise [Bentley, 2000], Prolog Website [Meridian Project Systems Corporation, 2000]

4.4 Access Control

Though the systems reviewed provide access control based on users' authorization levels, they assume that the user has been precisely identified, which is doubtful (as discussed earlier, in Section 4.1) since they use insecure password-based identification techniques.

4.5 Audit Trail and Assurance

Though some of the systems provide audit trail as a log that tracks a transaction participant's actions, it does not provide information about the reason why a particular document was approved by say, a project representative. An audit trail, including an intent of approval, is vital for conducting legally binding transactions since it can later be determined in court who the signer was, which document he/she thought he/she was signing, and what he/she intended for his/her signature to mean (did it mean he/she wanted to be legally obligated or did it just mean he/she wanted to show he/she had seen, though not necessarily approved, the document?) [Penop, 2000]. Also, currently none of the available systems provide any legally binding assurance to the users against post-transaction integrity. These systems do not provide assurance to the users that tampering of transaction data after a transaction has been committed would be detected in an acceptable manner, like invalidation of the transaction document.

4.6 Reliability of Infrastructure

The web based project management systems that were reviewed use public networks like the Internet to link the various organizations participating in large-scale A/E/C projects. Hence, users would be subjected to the bandwidth fluctuations prevalent in the Internet, affecting the reliability of these systems or in the extreme case hackers might make the system inaccessible i.e., a denial of service, for a length of time, as seen recently during the hack attacks on E-bay.com, Yahoo and CNN [CNN, 2000]. Thus, there is a need for a private communication channel within the Internet that is secure, reliable, economical to implement, and at the same time offers the wide accessibility of the Internet.

4.7 Scalability

Though most of the services reviewed were scalable in terms of technology and the kinds of projects they are applicable to, none of them were scalable to paper-based documents. If paper copies of electronic transaction data were made, the paper copies on their own could not be used to precisely identify the transaction participants in a legally binding manner.

4.8 Summary

To summarize, the security offered by currently available web based project management systems is limited as it doesn't address some of the most important security concerns of electronic transactions in large-scale A/E/C projects, as described in Chapter 3, effectively. The transactions conducted using these systems are also not legally binding due to the lack of transparency, precise identification of transaction participants, integrity of post-transaction data and effective audit control. Thus, there is a clear need to develop a framework for conducting secure and binding electronic transactions in large-scale A/E/C projects to build the much needed confidence among the A/E/C community to achieve a major of replacement of paper-based transactions. This framework could be used to improve security in existing project management systems or build new systems to facilitate secure and binding electronic transactions. The following chapter discusses the first step in the development of the framework namely, the development of the model for secure and reliable communication which would focus on the secure and reliable flow of information between the participants of a transaction through the integration of technologies like digital IDs for identification, non-repudiation and confidentiality, and virtual private networks for secure, reliable and economical connectivity.

Chapter 5

A Model for Secure and Reliable Communication

In order to build a framework for conducting secure electronic transactions, there is a need for a model that would provide secure and reliable communication, ensuring secure flow of information between the geographically distributed organizations participating in large-scale engineering projects. The following sections outline the three major components of a model that provides secure and reliable communication; namely, *authentication* for precise identification of transaction participants, *encryption* for confidentiality of transaction information, and *secure and reliable connectivity.* These sections also describe the technologies that need to be integrated within the framework to implement these components.

5.1 Authentication

To prevent impersonation during electronic communication, the origin of a transmission needs to be precisely determined by the recipient of the communication. In essence, we need to authenticate the sender of the transmission to its recipient. For example, consider

the case of a Change-Order being sent electronically to a contractor from the owner of a large-scale engineering project. The contractor needs to know that the transmission indeed came from the owner and not an impersonator; i.e. there is a need to authenticate the owner to the contractor through an authentication mechanism.

Authentication techniques that could be used for this purpose included secret-key cryptography systems like, Kerberos [MIT Project Athena, 2000] as well as, public-key cryptography systems like Digital IDs [Verisign, 2000]. Kerberos provides authentication through the use of tickets that are provided by a central authentication server on the network for each session after verifying the user's identity (that could range from a password, to a biometric measurement, like an iris scan). Since Kerberos removes authentication from the workstation, to a centralized authentication server on the network it would be ideal for use within a single organization, but in the case of a large-scale A/E/C projects where there are multiple organizations, it is not feasible to have an authentication server maintained by a particular organization, due to the inherent lack of trust between organizations. Thus, there is a need for authentication provided by a trusted third-party.

To provide authentication in the framework, it was decided to use digital IDs, which are an electronic means of verifying a sender's identity. Digital IDs use public key encryption techniques that use two related keys [Diffie and Hellman, 1976], a public key and a private key. In public key encryption, the public key is made available to anyone who wants to correspond with the owner of the key pair so that he/she can verify a message signed with the private key of the sender. Since the security of electronic messages signed this way relies on the security of the private key, the private key must be protected against unauthorized use. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached, and that the message has not been altered during transmission. When a message is digitally signed, it is sent through a hashing function that produces a message digest (compressed information about the document that uniquely identifies it). The message digest serves as the "digital fingerprint" of the message. This message digest is then encrypted using the

signer's private key, creating the digital signature that is attached to the message. If any part of the message is modified or corrupted during transmission, verification of the signature using the signer's public key will fail. The verification of the signature would also fail if the digital signature were not created with the signer's private key. Thus, digital IDs satisfy the requirements (see Chapter 3) of precise identification of transaction participants (and hence provides non-repudiation), as well as, that of maintaining the integrity of transaction information, during transmission of data (see Figure 5-1).

Digital IDs are provided by Certificate Authorities (CAs) like Verisign [Verisign Inc, 2000] or Entrust [Entrust Technologies Inc, 2000] after verifying the prospective owner's identity though his/her social security number, driver's license and/or credit card information. The Certification Authority notarizes an individual's or organization's right to use the key by digitally approving the digital ID after verifying the owner's identity. In a digital ID, the key pair is bound to a user's name and the other identifying information provided by the user like the social security number, driver's license and/or credit card information. The assurance provided by the digital ID depends on the trustworthiness of the CA [Laroche, 2000] that issued it and the integrity and security of the CA's practices and procedures [Verisign, 2000]. Since digital IDs are issued by trusted third-party organizations like CAs they are ideal for use in large-scale A/E/C projects where there is limited trust between organizations, unlike Kerberos where a ticket-issuing authentication server would have to be maintained by one of the organizations in the network.

Having discussed the advantages of using Digital IDs let us consider a scenario, in a typical large-scale A/E/C project, where Digital IDs can be used to provide authentication. Consider a situation where a project representative would like to send a Change-Order to a contractor using Digital IDs. The project representative would be in possession of a digital ID obtained from a particular Certificate Authority (CA), after his/her identity has been verified by the CA. He/She would then electronically sign the transmission containing the Change-Order form using his/her private key and send it to the contractor. The contractor can verify the authenticity of the project representative using the representative's public key that would be made freely available by both the CA

as well as the owner of the signature, in this case, the project representative. The success of the verification confirms both, that the person sending the document is the project representative and that the transmission was not modified in any way during transmission (see Figure 5-1). Thus, digital IDs provide a means to authenticate the sender of a transmission to its recipient, in essence, they provide precise identification of individual transaction participants (in this case the project representative to the contractor) and hence non-repudiation (the project representative cannot deny that the transmission was not sent by him/her since he/she signed it using his private key).

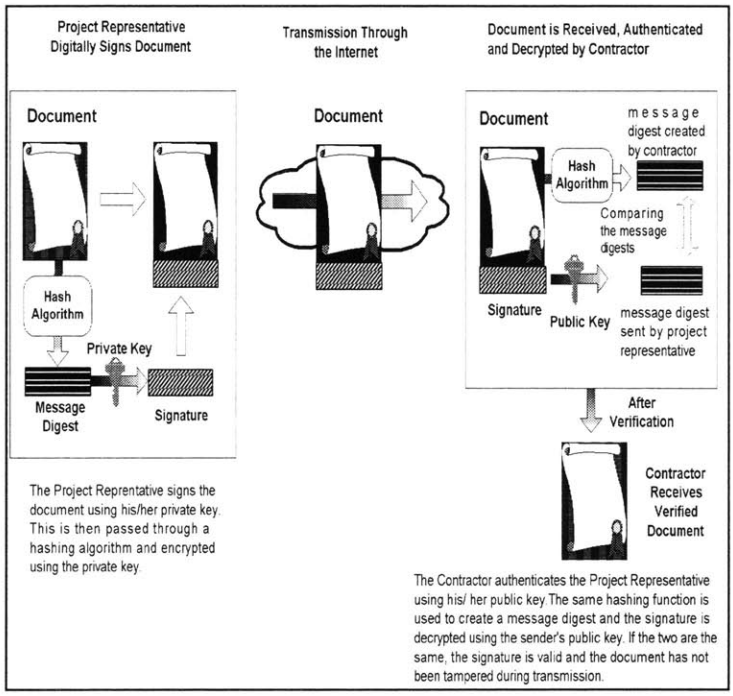


Figure 5-1: Authentication using Digital IDs

As it can be inferred, authentication is one of the building blocks of the model for secure and reliable communication required by the framework - it would uniquely identify individual transaction participants (and provide non-repudiation) during transmission of data. However, this component alone will not provide the necessary features, as defined in Chapter 3, to provide secure and binding electronic transactions in large-scale A/E/C projects. Another important requirement in the framework is to ensure that a document is

confidential during transmission. The next section provides information about encrypting transmissions after a document has been signed. Section 5.3 discusses the creation of a secure and reliable communication channel between the organizations involved in a large-scale project.

5.2 Encryption

Having integrated technology to satisfy the need for precisely identifying transaction participants (and provide non-repudiation) during data transmission into the framework, there is a need to provide confidentiality of transaction information within the framework. To stress the need for confidentiality, again consider the case of the Change-Order document being sent from an owner representative to a contractor. In the non-electronic environment it is sent in a sealed envelope from a project representative to the concerned person in the contractor's office, hidden from public view. Similarly, in the electronic environment there is a need for a technology that would hide the document from public view, during transmission. Digitally signing a transmission does not prevent it from being intercepted and read by someone other than the intended recipient. To ensure that only the recipient can read the transmission, it needs to be encrypted.

Encryption is a technique used to make information secure against intentional intrusion. It involves the transformation of information into an unintelligible form through the use of an encryption algorithm and a secret code known as the "key". The same "key", used in conjunction with the respective decryption algorithm, is required to decrypt the information. The size of the key determines the strength of the encryption performed. United States' laws allow encryption using keys up-to 128 bits in size (Center for Democracy and Technology, 1998) which according to RSA Labs [RSA Labs, 2000] would take a hacker *"trillion-trillion years"* to break. Thus, encryption can ensure data integrity or protect sensitive information sent over networks.

Encryption technology can be categorized as *secret key encryption techniques* and *public key encryption techniques*. Secret key encryption techniques use a single key to encrypt

and decrypt information and hence the key needs to be securely transmitted along with the encrypted information to the recipient, for decryption. Secret key encryption is suitable for an environment where the single key can be securely exchanged, for example, a small office where the key can be exchanged securely on a disk. However, it is not feasible to use secret key encryption in extranets, and over the Internet (as in the case of large-scale A/E/C projects), since it would compromise the security of the key during the exchange of the secret key [Atkins, Buis, Hare, 1997].

For large-scale A/E/C projects, it was determined that the use of public key encryption techniques like digital IDs (see Figure 5-2) is most appropriate. Since digital IDs are based on public key cryptography, the public key can also be used to encrypt messages that can only be decrypted using the corresponding private key. Because private keys cannot be derived from their corresponding public keys, public keys can be made widely available with no risk to security. For example, the contractor could obtain the project representative's public key from a directory service and use it to send him/her an encrypted message. Since the private key is never transmitted, public-key cryptography is suitable for insecure networks like the Internet. Though the use of public-key cryptography for encryption has the disadvantage of being slower than secret key cryptography, especially in the case of large data, the need for secure key management outweighs the need for high performance.

Hence Digital IDs used for authentication, as well as, encryption, provide a complete security solution by transparently maintaining the identity of all parties involved in a transaction [Verisign, 2000] (see Figure 5-2). Encryption provides the framework for secure electronic transactions with a technology to protect transaction information from public view, providing complete confidentiality, while digital signatures uniquely identify the sender of the information, providing non-repudiation, as well as, allow detection of changes made to the information during transmission. Having achieved identification and confidentiality during transmission of transaction information, the next key requirement the framework must satisfy is the ability to allow remote users in large-scale engineering projects to access the project network securely and reliably. For this

purpose the framework integrates technology that will create a secure and reliable electronic connection between geographically distributed organizations, as discussed in the next section.

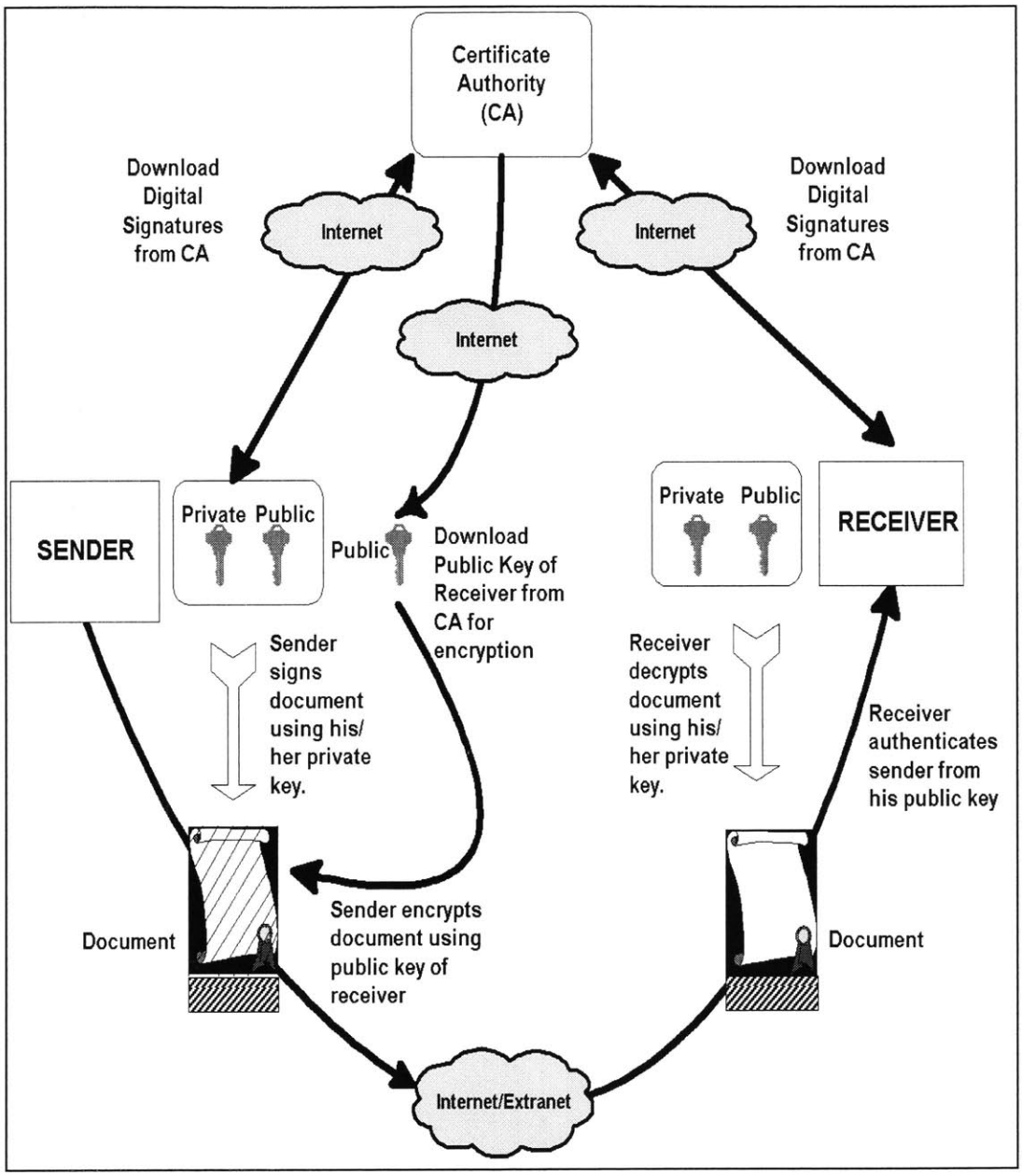


Figure 5-2: Authentication and Encryption using Digital IDs

5.3 Secure and Reliable Connectivity

Having integrated technologies for satisfying the requirements (see Chapter 3) of identification, non-repudiation and confidentiality during a transaction into the framework, there is a need to integrate a technology that provides a secure and reliable electronic connection between the organizations involved in a large scale A/E/C project, to allow remote users to connect to the project network securely and reliably, avoid exposing corporate data to unauthorized users and to provide a reasonable Quality of Service (QOS).

Due to the globalization of the construction industry the various participants of a large-scale A/E/C project could be located across the world. This rules out the possibility of a single corporate network that links all the participants in a large-scale project. Not only would each of the participating organizations have its own corporate network, which it would like to keep private to the organization as far as possible, but also a private project network linking all the organizations is not economically feasible. For this purpose, the framework integrates Virtual Private Network (VPN) technology that creates a communication channel providing a secure and reliable connection between geographically distributed organizations that is economically viable, and offers a reasonable Quality of Service (QOS), which for a VPN is defined [Cisco, 2000] as the ability to ensure prioritization of mission-critical or delay-sensitive traffic and manage congestion across varying bandwidth rates. A VPN would allow secure and reliable access from remote locations to a corporate network, for instance, when a contractor needs to access a particular contract's database inside the corporate network of the project.

A Virtual Private Network creates a "tunnel" through the Internet or other public networks, and provides the same security and features formerly only available on private networks. It allows a user working remotely to securely and reliably access a corporate server using the bandwidth provided by the public network. Thus, a VPN would allow the large scale engineering project's central office to connect to its field offices or other

participating organizations using a public network while maintaining a secure connection (see Figure 5-3 and Figure 7-2). From the user's perspective, the nature of the physical network is irrelevant because it appears as if the information is being sent over a dedicated private network.

The Virtual Private Network relies on the Point-to-Point Tunneling Protocol (PPTP) [Hamzeh, etal. 1999] that is an extension of the remote access Point-to-Point protocol (PPP) defined by the Internet Engineering Task Force (IETF) [Internet Engineering Task Force, 2000]. Since the PPTP protocol is included in environments like Windows NT and Windows 2000, users of computers running such an operating system can connect to a private network as a remote access client by using a public data network such as the Internet. PPTP uses Point-to-Point Protocol (PPP) authentication to validate the user credentials against, say, Windows NT and 2000 domains and the resulting session key is used to encrypt user data. Thus, it provides both authentication and encryption.

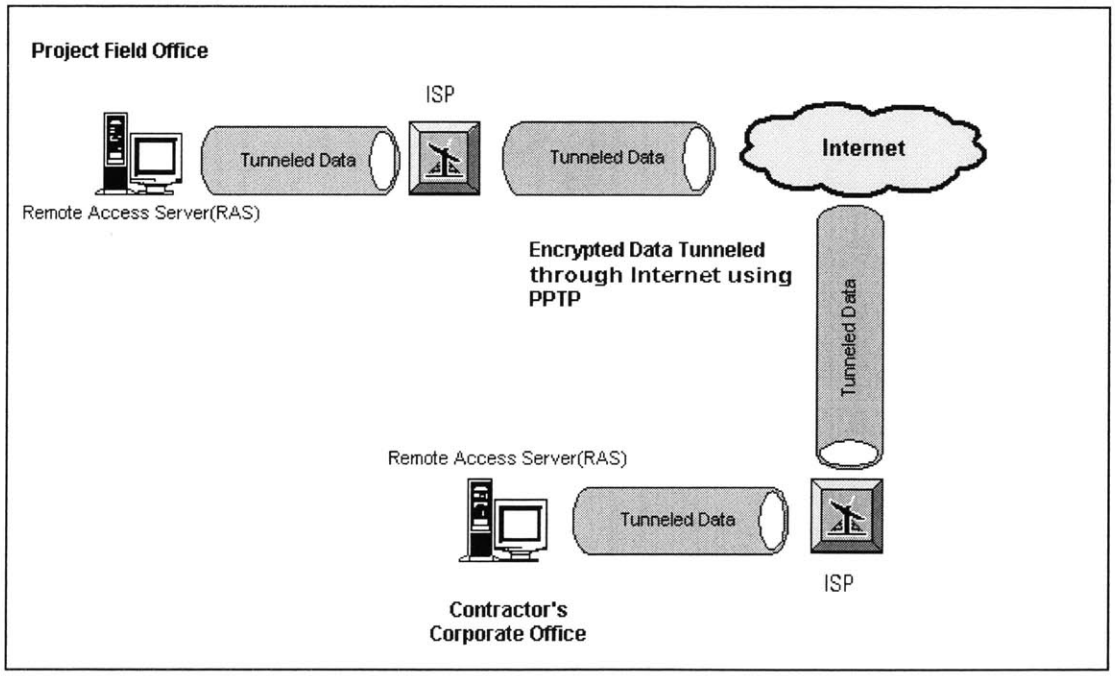


Figure 5-3: A Virtual Private Network

Though the VPN and digital IDs both provide encryption, they differ in the way they are implemented and the security concerns they address. Encryption in VPNs is done using keys created by the operating system (typically, the remote access server at an organization). Thus, a VPN provides encryption at the organization level and the success of the security provided depends on the trust the organizations have on one another. On the other hand, encryption using digital IDs is done using keys created by a CA (a third-party organization). This encryption is at the personal level and its success depends on the trustworthiness of the CA. Thus the framework requires both kinds of encryption as they complement each other by addressing different security needs: *organizational and personal.*

5.4 Summary

The integration of technologies that provide identification, non-repudiation and confidentiality, like digital IDs with virtual private network technology that provides secure and reliable connectivity creates a model for secure and reliable communication in large-scale A/E/C projects. This model forms the first step in creating a framework for conducting secure and binding electronic transactions in large-scale A/E/C projects. However, in order to truly achieve secure and binding electronic transactions in large-scale A/E/C projects, a model to securely manage transaction information after transmission is needed. This model would ensure the integrity of the transaction information beyond the life of the transmission (during transmission, the information is secured by the model for secure and reliable communication discussed in this section). The following section describes a model that integrates technologies like integrity checking algorithms, digitized signatures, and biometrics to securely manage transaction information, stored in the form of documents and databases, in large-scale A/E/C projects. These technologies would satisfy (or further strengthen) the requirements of identification, confidentiality, integrity, assurance, audit trail, access control and scalability as defined in Chapter 3.

Chapter 6

A Model for Secure Information Management

Having established, in the last chapter, a model for secure and reliable communication in large-scale A/E/C projects, the next major issue that needs to be addressed is the development of a model to securely manage transaction information (primarily in the form of documents) in large-scale projects. Most documents in a large-scale engineering project are of prime importance, because they are components of legal contracts between organizations. These documents are used to a large extent for claims and settlements during/after the project. Thus, it is of utmost importance that the information in these documents and the corresponding databases is secure. In the real (i.e., non–electronic) world, documents are primarily authenticated/secured using handwritten signatures. These documents make the parties involved (i.e., owners, and contractors) accountable for the commitments made in the documents, and are routinely used as valuable evidence in legal claims/settlements. In order to truly replace paper-based documents, through a

transition to the electronic environment, the framework would require technology that not only allows electronic approval of transactions, prevents tampering of electronic information but also has legal standing i.e. non-repudiation during claims.

The model for Secure Information Management, discussed in this section, focuses on the secure storage, retrieval and management of transaction information, in the form of electronic documents and databases, before and after it has been transmitted between transaction participants. Though digital IDs ensure integrity of transaction information during the transmission of data they do not secure data before or after transmission. In order to securely manage transaction information by addressing the issues of identification, integrity, access-control, audit control and assurance as defined by the requirements in Chapter 3, technologies like integrity checking algorithms, digitized signatures and biometrics have been integrated into the framework.

6.1 Integrity Checking Algorithms

A solution to the problem of securing electronic information after a transaction has been committed is the use of "integrity-checking algorithms", to create a unique fingerprint of the original transaction information, which could be used to differentiate original transaction information from modified versions. The most popular integrity-checking algorithm (also known as one-way hash functions) is the MD5 checksum algorithm [Kaliski and Robshaw, 1995] developed by RSA [RSA Data Security Inc., 2000] that calculates a checksum of the information that needs to be secured. A checksum is the equivalent of a "fingerprint" (a series of bits) for a chunk of information. The larger the size of the checksum used by the algorithm the smaller the chances of two different sets of information having the same checksum. The framework developed in this research effort adopts the use of 128 bit MD5 checksum algorithms for maximum security.

Integrity-checking algorithms like MD5 can be used to detect tampering of information once it has been validated; hence they can be used to secure transaction information. At any point of time after validation, the checksum for the information can be calculated and

compared to the original checksum. A difference in the checksums indicates that the information had been modified. Thus, while digital signatures ensure that information is not read or modified during transmission, integrity-checking algorithms ensure that the information is not modified after receipt. In essence, integrity-checking algorithms provide the participants of a transaction with the assurance that any attempt to tamper with the information after a transaction would be detected.

In order to protect the information in documents after they have been approved, the checksum needs to be calculated at the time of approval, so that any change made to the document after the approval would lead to the failure of the verification of the checksum. This logical requirement that the act of approval needs to be linked to the act of checksum calculation is met by the use of digitized signatures for the approval of documents, as described in the next section.

6.2 Digitized Signatures

Interviews with professionals involved in transactions in large-scale engineering projects led to an important requirement in the transition from paper-based transactions to electronic transactions. There was a need for a signature that is visible and easily recognizable on electronic documents, similar to handwritten signatures. A "Digital" ID (discussed in Section 5.1) is not a handwritten signature bound to a document, but a numeric code related to the document, that validates its contents upon receipt and opening of a transmission. If paper copies of a document are required, there will be no way to validate its originality. Though digital IDs identify transaction participants during transmission of transaction information, in order to identify them in a manner that is scalable to paper-based transactions (as defined in the requirements in Chapter 3) the framework requires a technology that imbeds handwritten signatures into documents electronically.

"Digitized" signatures are the electronic equivalent of handwritten signatures that can be embedded into documents. A digitized signature is not just the graphical representation of

a handwritten signature - along with the graphical representation of the signature; it contains the biometric measurements associated with a signature, the checksum value of the information that was approved, as well as, the intent of the signatory while signing the document [Penop Inc, 2000]. While the biometric measurements, uniquely associated with a person, would make forgery of signatures extremely difficult, the intent of the signatory stored in the signature (also recorded as part of the audit trail for the transaction) would provide legal digital evidence for the occurrence of the transaction. Digitized signatures are being evaluated as a legal alternative for handwritten signatures in several states [Perkins Coie LLP, 2000] and hence would provide non-repudiation in the case of legal claims. Thus, through biometric technology, digitized signatures provide the framework with an equivalent, albeit more secure, alternative to handwritten signatures.

6.2.1 Biometric Security

Biometric verification is a method by which an individual's identity is confirmed by examining a unique physical trait or behavioral characteristic, such as a fingerprint, retina, palm print or voice. Unlike a password or Personal Identification Number (PIN), a biometric trait cannot be lost, stolen, or recreated. According to a study conducted by the Gartner Group [Gartner Group, 1999], biometric security has been forecasted to be a key component for security systems of the future because they are based on characteristics unique to a person, making forgery or misuse extremely difficult. The framework developed in this research effort integrates biometric technology in the form of digitized handwritten signatures. Apart from using biometric security techniques like digitized signatures as a replacement for handwritten signatures, the use of biometric technologies like finger print, voice detection, iris scan and face recognition are also being explored for maintaining access control in the transaction management systems since they are more secure and convenient as compared to non-biometric techniques like the use of passwords. The diverse range of biometric technologies would not only allow users to choose from a range of identification mechanisms based on availability and convenience,

but also create the redundancy needed in this application to minimize the impact of failure of a particular identification device.

In the case of digitized signatures, typical biometric measures include the stroke direction, order, acceleration, and deceleration to name a few. For the framework, the digitized signatures developed by Penop Inc. [Penop Inc, 2000] were used. This biometric signature based security system consists of a biometric token that is uniquely associated with each signature. A biometric token is a fully portable, encrypted data item that encapsulates the unique characteristics of a signature together with information about the signatory and the reason for signing [Penop Inc, 1999]. The signatures itself are stored as a set of measures, each representing a unique characteristic. The original signature data is not stored since this would increase the risk of forgery, but the token stores sufficient information to render the image on a graphic display. Penop™ [Penop Inc, 1999] has identified some of the properties a biometric token needs to have, namely,

Identity: The name of the signatory, or other unique identifier such as e-mail address.
Timestamp: The date and time the signature was written, together with hardware identification.
Document Checksum: Linking the individual act of signing to a single document to prevent signature re-use, using the MD5 checksum algorithm.
Signature Measures: Forty-three biometric measurements of signature behavior: e.g. stroke direction, order, speed, acceleration and deceleration of pen, pen pressure, off writing surface time.
Signature Image: For rendering the image.
Verification from Signature Database: The signature can be verified from an online database of signatures, comparing biometric measurements.

As required by the framework, the digitized signature from Penop Inc provides a link between the actual act of signing and the information in the document being approved by the signatory by imbedding the checksum value of the information into the signature

(using the MD5 checksum algorithm). Thus, at the time of signing, the signature is automatically bound to the contents of the document.

Digitized signatures add value to the framework in four ways. Firstly, it complements Digital IDs in precisely identifying transaction participants. While Digital IDs identify transaction participants during the transmission of transaction information between participants over the network, digitized signatures are used to identify transaction participants after the transaction has been committed, say when an electronic copy of the transaction is viewed on a computer or when a paper copy of the transaction document is made for use during claims. Biometric digitized signatures are extremely difficult to forge and hence along with Digital IDs they precisely identify the participants of a transaction as required by a framework.

Secondly, digitized signatures help maintain the integrity of transaction information by storing a checksum of the information that has been approved by that particular signatory and hence binds the data to a signature. The integrity of the data can be verified at any time by comparing the checksum stored in the signature with the checksum of the data. They also provide assurance (as required by the framework) that if the integrity of the transaction information is lost, the corresponding signature on the document is invalidated.

Thirdly, the digitized signatures, from Penop [Penop, 2000], which were used in the framework collect an "intent of approval" from the signatory before the signature is embedded in the document. This "intent of approval" provides legal electronic evidence for an approval in a transaction (hence making the transaction more binding legally) and is also useful for maintaining a more effective audit control for the entire transaction, as required by the framework.

Lastly, digitized signatures (and not any other biometric technology) provide the crucial link between the electronic and non-electronic world. Since ages, people have viewed handwritten signatures in documents as a legally binding identification mechanism and

have used it to provide non-repudiation in legal claims. Thus the use of digitized signatures in this framework would not only provide precise identification of participants and non-repudiation but would also ease the transition for corporations from paper documents to electronic transactions since digitized signatures are in essence, handwritten signatures, albeit considerably more secure.

To summarize briefly, the model for secure and reliable communication developed in Chapter 5 focuses on securing transaction information, during its transmission between organizations, through the use of Digital IDs and VPN technology that provide identification, confidentiality and secure, reliable and economical connectivity. On the other hand, digitized signatures, based on biometric technology, complement the secure and reliable communication model, by providing the framework with a means to secure transaction information, by identifying transaction participants using a unique human trait, maintaining data integrity, providing assurance and an audit trail. Having identified the value of technologies like integrity checking algorithms, digitized signatures, and biometrics, they are integrated into the framework, to secure information stored in documents (in Section 6.3) and in databases (in Section 6.4).

6.3 Securing Documents

The primary source of information in large-scale A/E/C projects are documents, ranging from contractual letters, CAD drawings, schedules to spreadsheets. These documents can either be stored electronically using document management systems or the information in them can be extracted and stored in the projects' database management systems. The latter approach leads to the physical separation of important - or frequently used – information, however it improves the organization of data, leading to faster search and retrieval using a database management system. Thus, the information in a large-scale project can be divided into two broad categories, that which is in the form of documents (stored in document management systems) and that, which is organized in database management systems.

In the framework, digitized signatures are used to secure both categories of information in large-scale engineering projects – documents and databases. For documents, two possible ways to secure the information have been identified. Firstly, a biometric signature plug-in could be developed for each of the software systems used. For example, a plug-in for Microsoft ™ Word has been developed by Penop Inc. for letters [Penop Signature Plug-in for Microsoft ™ Word, 1999] and for PDF documents [Penop Signature Plug-in for, Adobe Acrobat™, 1999]. In this way the documents can be approved directly, from within the software systems. Upon approval, the signature along with the checksum value would be embedded securely into the document, allowing a check for tampering of information after the document has been approved. Though, this is probably one of the best solutions, a major disadvantage to this technique is perceived – a separate plug-in has to be developed for each document system increasing the cost of development and use depending on the program used in a corporation. Thus, it's use and availability will be usually limited by program popularity in the consumer market and not necessarily in a specialized market such as Civil Engineering.

The second technique, which the framework uses to secure documents, is through the development of a File Approval System (FAS). This application was developed using Visual Basic [Smith, Whisler and Marquis, 1998] and the Penop ActiveX API [Penop SDK documentation, 1998]. This application can be used to approve any kind of file (e.g. letters, schedules, CAD drawings, audio/video clips) using the digitized signature of the approver. The user is allowed to select the file he/she wishes to approve and signs on a digital pad or hand-held device. At the time of approval the following details are also captured and bound to the signature – name of the approver, date and time of approval, the intent of approval and the checksum of the contents of the file. If any change is made to the file after it has been approved, the checksum associated with the signature of the person that approved the particular file also changes. At any point in time, the integrity of the file can be checked by verifying the signatures (i.e., double-click on the signature). If the file has not been tampered after approval, the user is informed that the file hasn't been tampered with (see Figure 6-1).

At the same time, the system provides assurance that if the file was modified, the user is informed that the file has been changed after it had been approved (see Figure 6-2). Though, this application has the ability to approve any kind of document (i.e., file), provides identification of transaction participants, maintains integrity of transaction data and provides assurance and an audit trail it has the disadvantage that the signature is not imbedded into the document that is approved (unlike the plug-ins). The signature of approval is stored in a separate file (not in the document file) and hence, if the signature file is deleted, the verification cannot be performed. Nonetheless, as long as the document remains in electronic form and verification is done through the FAS, there is no problem verifying any kind of document, but if the document has to be printed for legal purposes then the lack of the signature on the document can be a major drawback because the paper copy would not have a handwritten signature on it to verify the approval of the document. The solution adopted in the framework for this problem is the use of a cover page (similar to a cover page used in certain types of internal documents in A/E/C projects) containing information about the file – like name, location on the file server, size and some key features extracted from the file - and the signature of the approver. This way the paper copy of the document is related to the process of approval by filing the cover page and the document together. Thus, there is a tradeoff between general availability and document dependency.

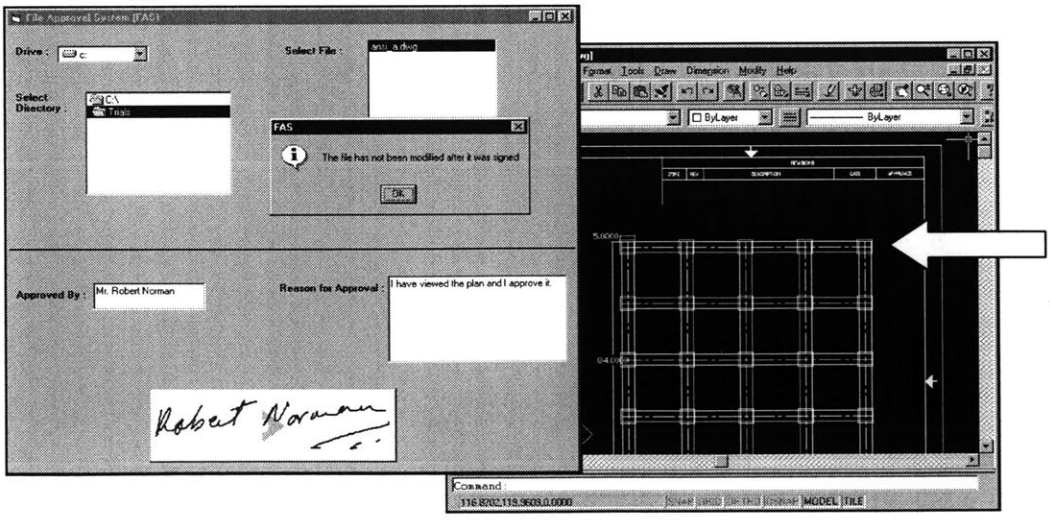


Figure 6-1: Validation of an approval of a CAD Drawing – It hasn't been modified after approval.

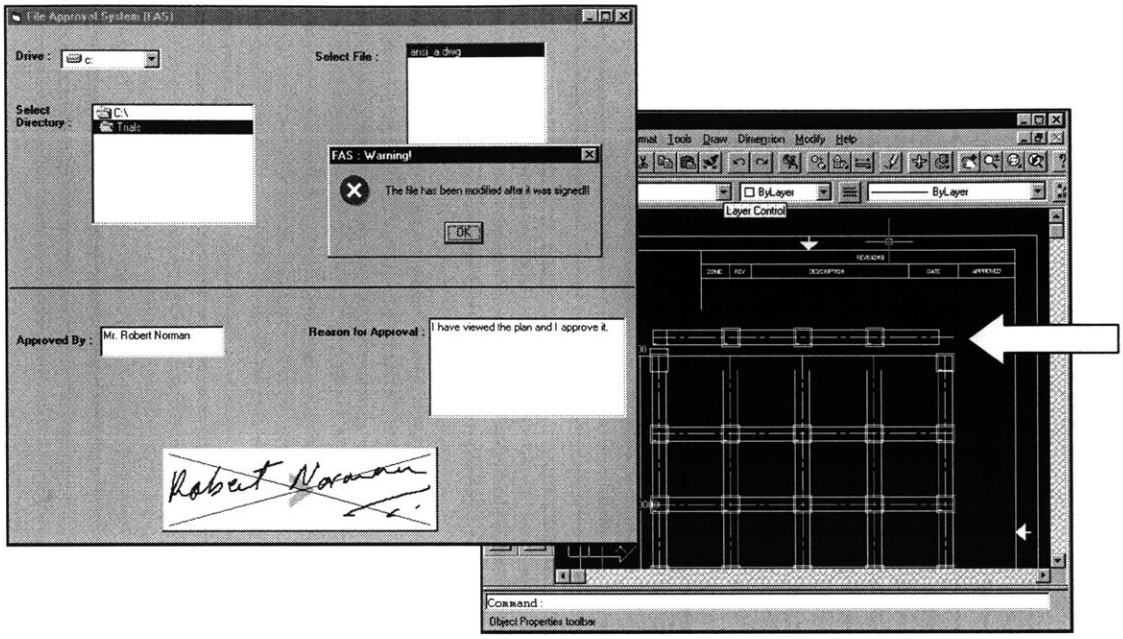


Figure 6-2: Invalidation of approval after the CAD Drawing has been modified (wall moved away).

Having integrated integrity-checking algorithms and digitized signatures into the framework, to allow electronic approval of documents and to maintain integrity of transaction data stored in documents, these technologies are now extended to maintain the integrity of transaction data that is extracted to databases (from documents) through the development of a Document Approval System (DAS).

6.4 Document Approval System

To automate the process of document approval and maintain integrity of transaction data stored in project databases, a Document Approval System (DAS) has been developed. The DAS allows the approval of a document electronically securing its content and stores the information in the project database for future retrieval. A client-server based prototype system (see Figure 6-3) has been developed using Visual Basic [Smith, Whisler and Marquis, 1998], Remote Database Objects (RDO) Library [Lassasen, 1998], the

Penop ActiveX API [Penop SDK Documentation, 1998] and a relational database system (in this case, Oracle Server [Oracle Server Documentation, 1998]).

This prototype allows the approval of a Change-Order in a project. In this system, change-orders are initiated by the project representative at a construction site to indicate/ address a previously unperceived condition (see Figure 6-3). The contractor has to respond within a fixed period of time (indicated in the change order form) with a proposal for the change to be executed. It then needs to be authorized by representatives of the project and federal/state government (in case, of a public project like the Central Artery/Tunnel Project at Boston).

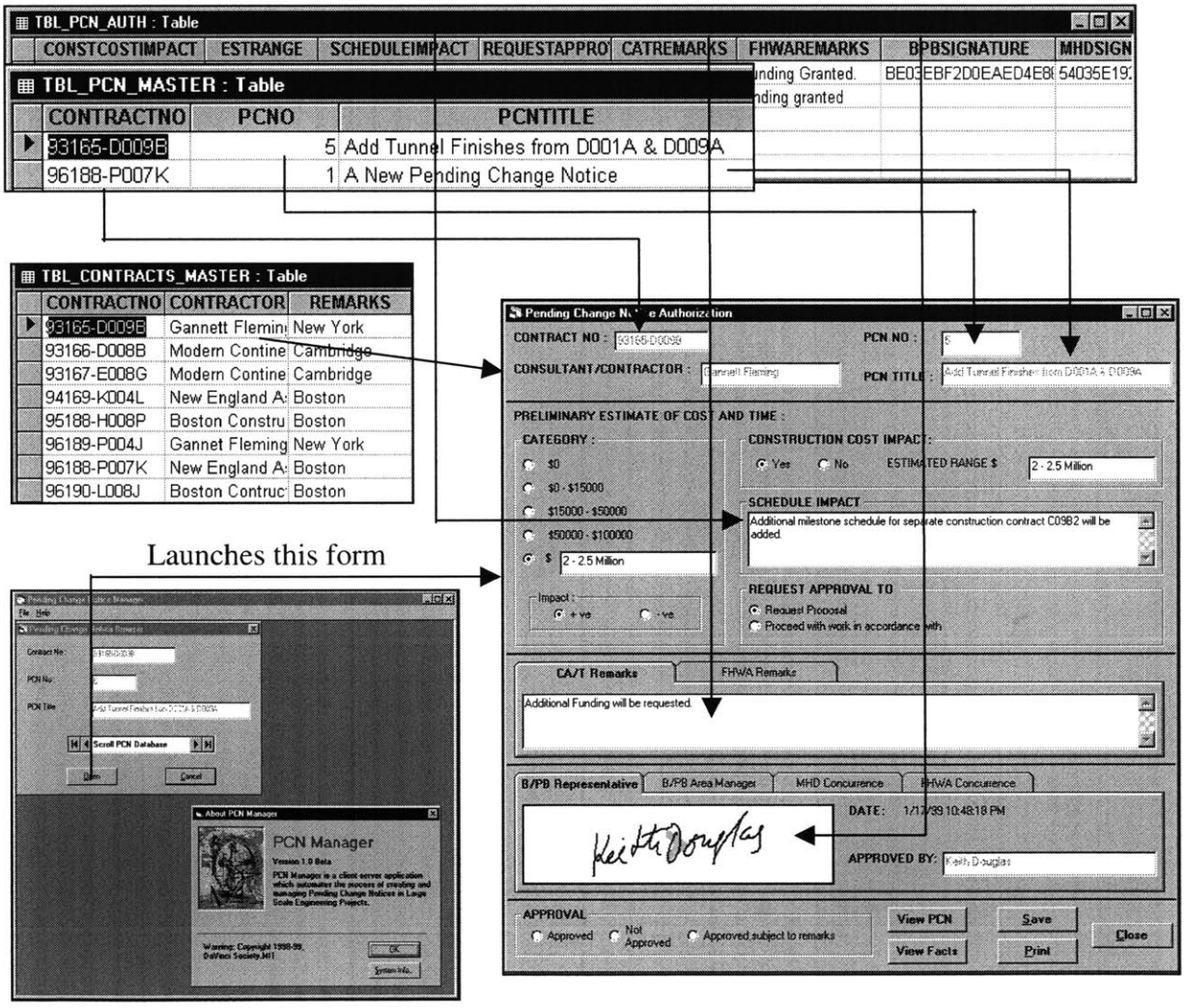
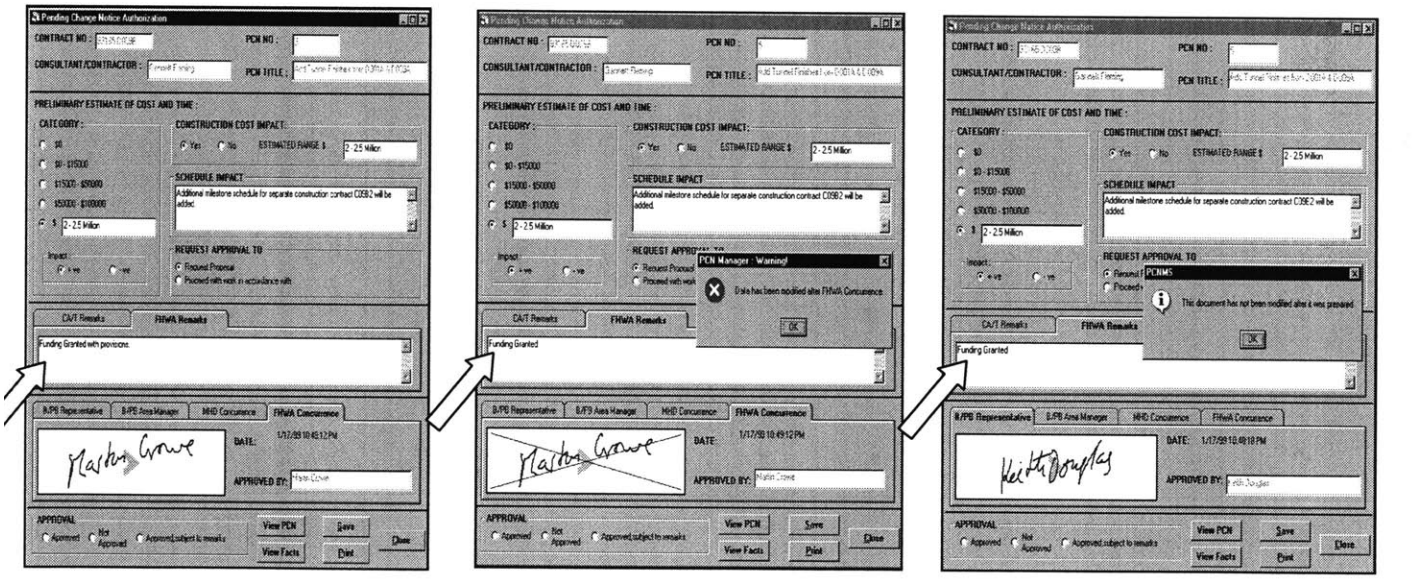


Figure 6-3: The Pending Change Notice Authorization Form and a snapshot of the database (Note: the signature is encrypted and stored in the database)

The prototype allows the project representative to create a Change-Order request using an interactive GUI. Once the Change-Order request is created, he/she approves it electronically and then the remaining authorities (area manager and state/federal representatives) can view or approve the change order. Each signature of approval is associated with the information that was approved by the particular authorizing agent. For instance, the comments of the state and federal representatives are not associated with the approval (i.e., signature) of the area manager or the project representative. Thus, a change to these fields would invalidate the signatures of the state and federal representatives but not those of the area manager and the project representative (see Figure 6-4). This is because the area manager and the project representative approved the document before the state and federal representatives and hence the validity of what they approved is not affected by the comments of the state and federal representatives.



Original form with FHWA Approval

A Modification to FHWA remarks invalidates the FHWA approval

A modification to the FHWA remarks doesn't invalidate the Project Representative's approval.

Figure 6-4: Pending Change Notice Forms

The information in the form is extracted to the project database along with the signatures when it is committed. The signatures are converted into encrypted text before they are

stored in the database. Any change to the information in the database (either through this application, or otherwise) invalidates the corresponding approvals as soon as the form is reopened or printed.

The application, named, the "Pending Change Notice (PCN) Manager", has an interactive interface which allows users to scroll through the existing pending change notices in the database, or create new notices. To achieve database independence, the system has been developed using Microsoft's Remote Data Objects (RDO) [Lassasen, 1998] that uses the ODBC interface to provide database independent connectivity [Geiger, 1997]. As an improvement to the original system and for application on the test case (see Chapter 7), a web-enabled version of this application, that allows project managers to approve documents through a browser interface (see Figure 6-5), has also been developed, as part of a workflow system [Li, 1999]. This version also supports online verification of the approvers' signatures from a database of authorized signatures before attaching the signature to the document, to secure the system against forgery. This is crucial in a web-based system since it would be more widely accessible than a client-server system, requiring more security.

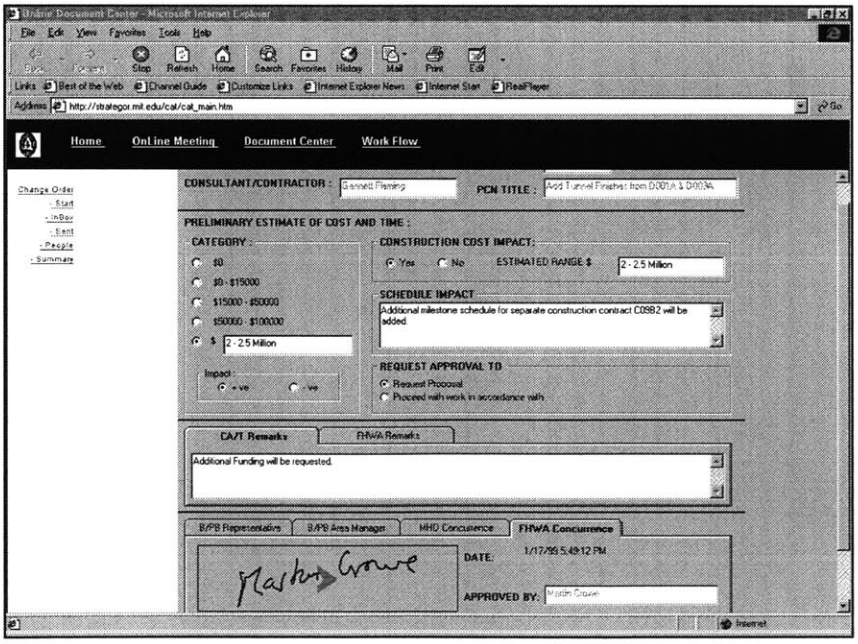


Figure 6-5: Web enabled version of Document Approval System (DAS)

6.5 Summary

In summary, the model for secure and reliable communication, discussed in Chapter 5, ensures secure information flow between the geographically distributed organizations participating in an A/E/C project by providing the framework with identification of users, confidentiality and secure and reliable connectivity. While identification and confidentiality is provided through the use of digital signatures, secure and reliable connectivity is achieved through the use of virtual private networks. On the other hand, the model for secure information management, discussed in Chapter 6, ensures integrity, non-repudiation, audit-trail, assurance and access-control of transaction information, stored in documents and databases, during, as well as, beyond the life of the transaction, through the use of technologies like integrity-checking algorithms, digitized signatures and biometrics. Having developed the models for secure and reliable communication and secure information management as required by the framework, the next chapter discusses the issues related to the implementation of the framework in an IT initiative at the $ 13.6 Billion Central Artery Tunnel (CA/T) Project in Boston, USA.

Chapter 7

Case Study: Central Artery/ Tunnel (CA/T) Project, Boston, US

The $13.6 billion Central Artery/Tunnel Project [CA/T Project, 2000] is the largest and most complex highway project in American history - it is larger than the Panama Canal and the Alaska Pipeline (if these projects' final budget were put in 2004 dollars, when the Artery project will be finished). In late 1998 the construction work force was about 2,700 workers. Designers, construction managers, and other support personnel brought the total to about 5,000 people employed full time by the Central Artery project and its contractors. At the peak of construction employment in the year 2000, about 4,000 construction workers are expected to be employed on the project. The cost of the project is shared by the Federal government, which will pay about 70 percent of all costs by the time work is finished, and the Commonwealth of Massachusetts, which will pay about 30 percent.

The project (see Figure 7-1) includes two main elements -- the extension of Interstate 90 (the Massachusetts Turnpike) from its current terminus south of downtown Boston under Boston Harbor to Logan Airport, and the replacement of Interstate 93 through downtown Boston, including a tunnel through the heart of the city. Other major elements include, four major highway interchanges; a two-bridge, 14-lane crossing of the Charles River on the northern edge of downtown Boston; the world's largest highway tunnel ventilation system; the world's most advanced electronic traffic management and incident response system; demolition of the existing elevated Central Artery (I-93) downtown; and 150 acres of new parks and open space, including 27 acres downtown where the elevated Central Artery now stands. An important feature of the project is keeping the city of Boston open for business throughout more than a decade of construction, which involves (among many other things) holding up the six-lane elevated highway while tunneling for an eight-to-ten-lane underground expressway directly underneath.

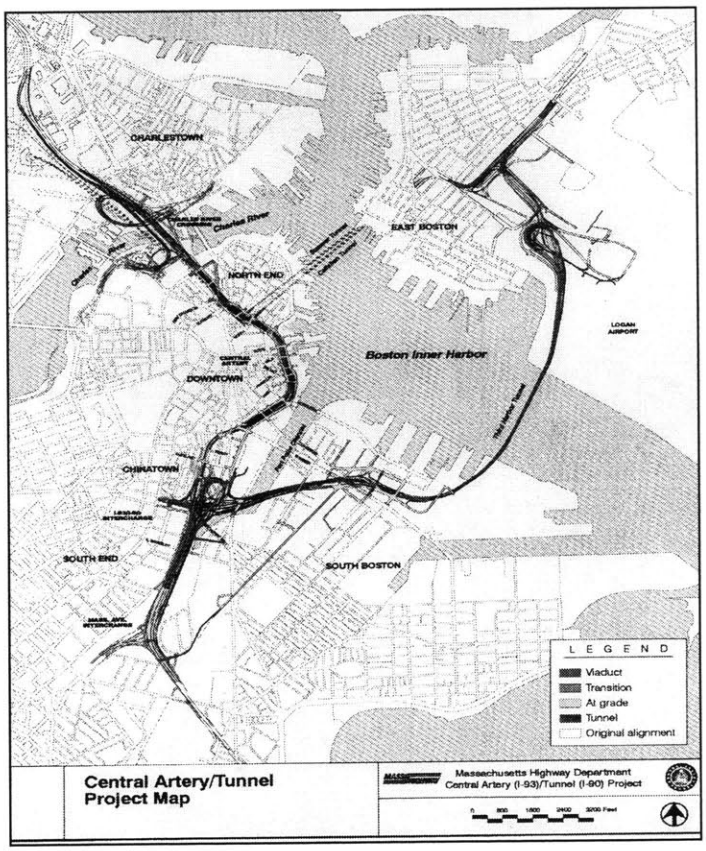


Figure 7 –1: The Central Artery/ Tunnel Project in Boston, USA (CA/T Project, 2000)

7.1 The IT initiative at the CA/T Project

Since the commencement of the Project, there has been a commitment in the Project to effectively use information technology (IT) to improve productivity and performance. During the design stage, there was immense application of IT in the form of Computer Aided Engineering for such tasks as 3D modeling, 4D CAD and simulations. For the construction stage, initially, the Project used independent commercial project management systems like Primavera P3 [Primavera Systems Inc, 2000], Timberline [Timberline Software Corporation, 2000] and Expedition [Primavera Systems Inc, 2000], but in 1993 they introduced an Oracle-based [Oracle Corporation, 2000] information management system to improve data consistency and control on both the design and construction stages. This move was well accepted in the project after receiving unconditional support from top management in the project, as well as great support, from both the IT and construction departments of the Project. Introducing a commercial database system like Oracle has helped extract data from documents and forms in proprietary format to industry standard databases. This has not only helped in collecting and retrieving data efficiently, but has also helped reduce turn around time in making project decisions since management has instant access to project data.

Now, at the peak of the construction stage, the Project is in the process of building on their Oracle based Information Management System to reach not only project personnel but also the large population of the contactor. In order to achieve that, the project is developing a "paper-less" office with an aim to reach the stage in which all project data and transactions (between all project participants) are electronic. Apart from providing greater transparency, this would help reduce the number of file cabinets, containing project documents, which need to be turned over to the State at the completion of the project. The "paper-less" office is being developed by the IT department at the CA/T Project [CA/T Project, 2000] and Modern Continental Companies Inc. [Modern Continental Companies Inc., 2000], with research support from MIT. To reduce the risk of a full-scale investment by making the whole project "paper-less" (and not "paperless" because the aim is to reduce paper, not eliminate it completely) simultaneously, it was

proposed to first implement a test study on the $140 million I-93-Storrow Drive Connectors construction contract (i.e., C19E1- Contract). Based on the performance and success of this test office the paper-less office effort would be extended to the other contracts in the CA/T project. In the process of creating the "paper-less" office, one of the biggest challenges faced was that of conducting secure and binding electronic transactions between the project participants, in this case the project representative in the field office and the contractor. This challenge was planned to be overcome by implementing the security framework, described in this thesis, that address the security concerns (see Chapter 3) in conducting secure and binding electronic transactions in A/E/C projects.

7.2 Secure and Reliable Communication at the CA/T Project

Based on the secure and reliable communication framework (Chapter 4), an extra-net plan (see Figure 7-2) was developed for the CA/T project test office. The CA/T central office is currently connected electronically to the field offices of the various contracts using frame relay systems. The plan called to connect the test office to the contractor's (i.e., Modern Continental Companies Inc) project office in three possible ways (in order of preference of use) to achieve a great level of redundancy. Firstly, a high-speed T-1 line was to be used to connect the offices to increase speed and reliability. Secondly, a Virtual Private Network (VPN) was to enable secure remote access between the contractor's project office and the field office through the Internet. Lastly, the offices were to be connected using a telephone line/modem. The T-1 line was the fastest and most reliable connection but it's also the most expensive. The Virtual Private Network and phone lines/modems offer relatively lower performance but were more economical options. These three connections would provide ample redundancy to tackle a possible failure in one of the above communication channels.

In this architecture, a typical transmission, from the project representative, would be digitally signed and encrypted by him/her (using his/her private key) and sent through the Virtual Private Network (where it would be encrypted again using a key created by the

operating system of the receiving organization for the transmission) to the contractor's project network. As explained earlier (Section 5.3), while the encryption in the VPN provides secure communication between trusted organizations, the encryption provided by the digital signatures secure the transmission between individuals, creating a truly private communication. The Remote Access Server (RAS) at the contractor's office would authenticate the project representative and send the transmission to the recipient. The recipient not only decrypts the transmission using the public key of the project representative but also authenticates the sender (project representative) of the transmission.

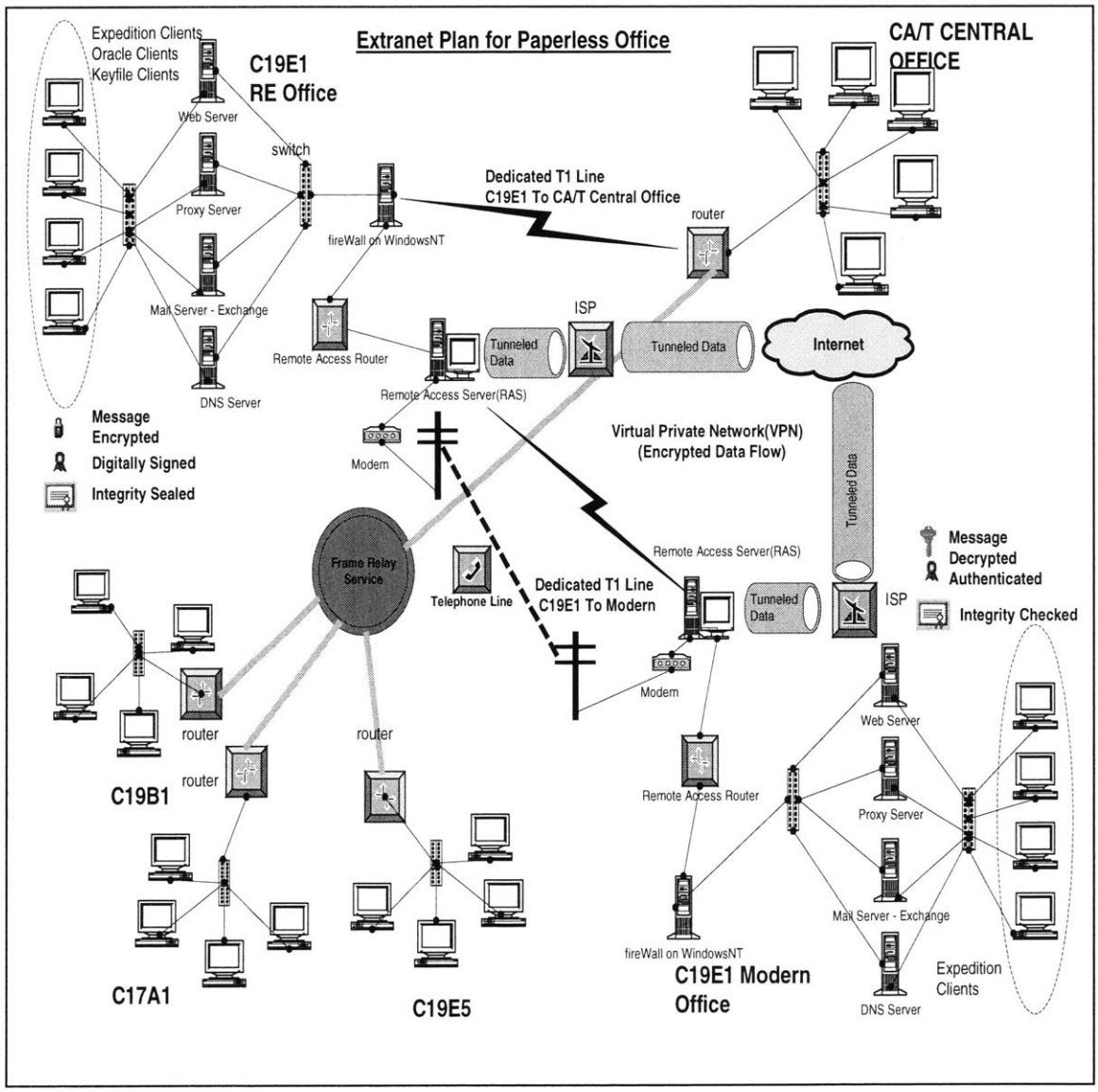


Figure 7-2: Extra-net architecture at the CA/T Project

Having developed an extra-net plan, based on the model for secure and reliable communication, to the Central Artery Tunnel Project, an architecture that would enable secure management of transaction information (based on the model for secure information management discussed in this thesis, i.e., Chapter 6) was also developed.

7.3 Secure Information Management

In order to securely manage information, the model for secure information management (described in Chapter 6) in the form of an integrated *Web-based Secure Document Approval System Architecture* (see Figure 7-3) was implemented. The system consisted of web-based clients (ASP documents embedded with ActiveX components/objects) to digitally approve documents (see Figure 7-3), as well as, to digitally verify their authenticity/integrity through a web browser. The web-based clients reduced the problem associated with distribution of newer versions of client software, currently prevalent in the Project. The web-based infrastructure allowed latest versions of the software to be immediately available to users across the Project.

The system extracted transaction information to the project and contractor databases from the forms to ensure persistence of information beyond the life of the transaction. In this application, there was a need for separate databases (with replication) for each organization (the Project and the contractor) because of security and trust concerns. Hence, the contractor as well as the project had separate databases where they had their own copies of transaction data. Since most organizations preferred using their existing corporate database systems, the system was database independent. Hence, all database communication was through a database independent interface provided by the *Active Data Objects (ADO^{TM})* [Smith, Whisler and Marquis, 1998].

As defined in the framework proposed in this thesis, the first step towards achieving secure and binding electronic transactions was to provide secure communication, to satisfy the need for identification, non-repudiation, integrity and confidentiality during transmission of transaction information. In order to achieve this in the integrated *Web-*

based Secure Document Approval System Architecture, there was a need for a component in the architecture that would encapsulate services to satisfy these requirements of secure communication. A *secure communication object* developed using the Microsoft Crypto API [Microsoft Corporation, 2000] implemented the secure communication model discussed in Chapter 5. This object provided authentication and encryption services through Digital IDs from Verisign [Verisign Corporation, 2000] while the Remote Access Service (RAS) for Windows NT provided virtual private network technology for secure and reliable connectivity, as required by the model.

Having created a component for secure communication, the next step was to secure transaction information before and after it had been transmitted across the network. This was achieved by developing components that encapsulated the services of integrity checking algorithms, digitized signatures and biometrics within the document-approval architecture. The *digitized signature objects* allowed online approval, verification of document integrity, assurance, intent of approval while the *security interface* controlled access to the system using biometric verification of fingerprints, faces as well as traditional password/smart-card based security. A DCOM based *security server* provided security services to both the *signature objects* as well as the *security interface* through security databases. While a *signature database* containing the "digitized" signatures of all the possible approvers was used to verify an approver's signature as soon as he/she signs the form, fingerprint and facial information databases were used for bio-metric verification at the *security interface* (see Figure 7-4).

To prevent misuse of security information like signatures and fingerprints, these databases were distributed among the different organizations. Due to security concerns, unlike the primary transaction databases, these databases were not replicated. Each organization's security databases contained data for the users who belong to that particular organization since the Project would not like the contractor having a database of the signatures of its representatives and vice-versa. A prototype of the integrated system, based on the framework for secure and binding electronic transactions explained in this thesis, has been implemented for the test case.

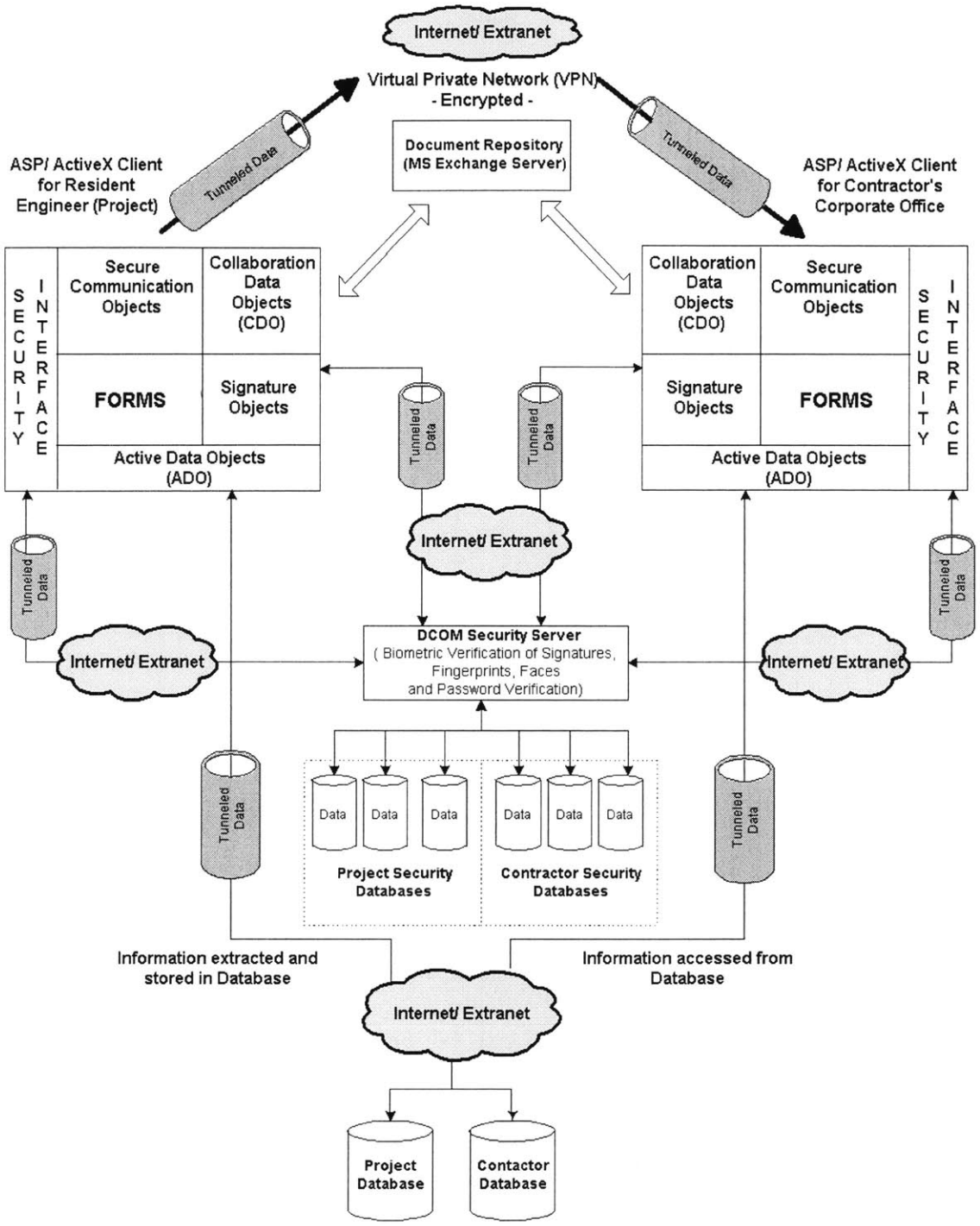


Figure 7-3: Integrated Document Approval System Architecture

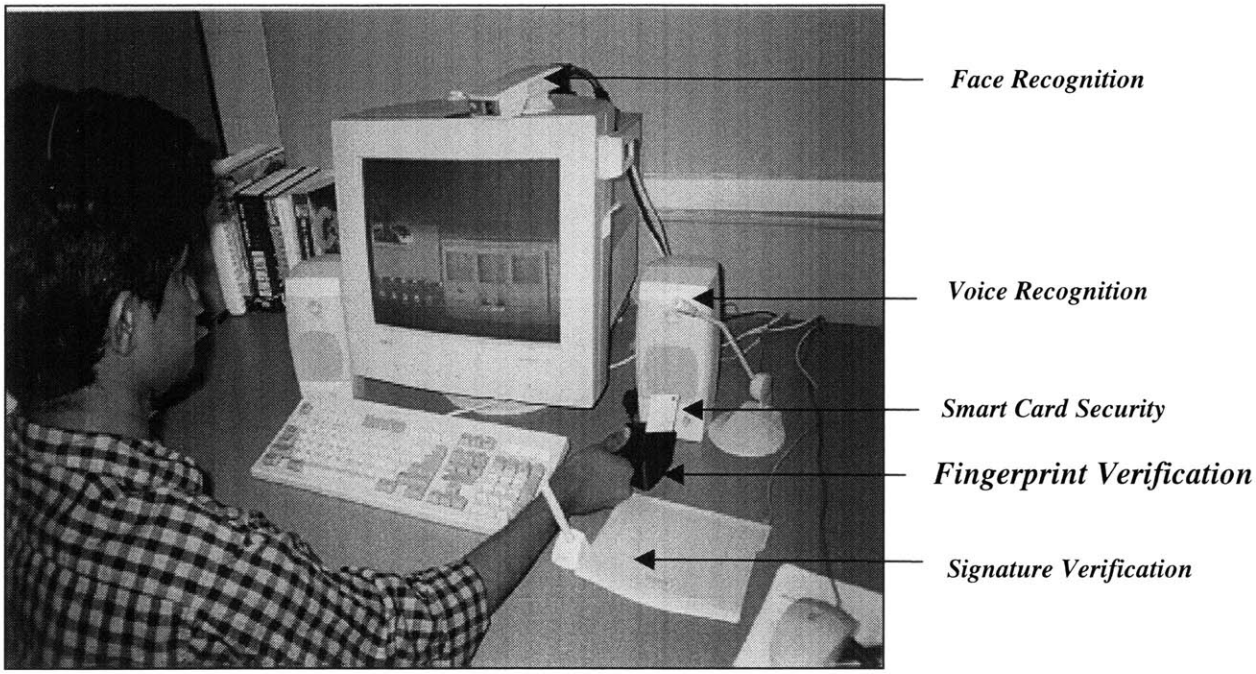


Figure 7-4: Biometric Devices

7.4 Paperless Office Implementation - Analysis of Benefits and Results

The development status of the paper-less test office (in Contract C19E1) at the Central Artery Project was evaluated from time to time by the Project's IT Task Force (which included researchers from MIT). Three major status checks were conducted during the course of the development of the paper-less office – A preliminary analysis at the start of the implementation in September 1998, a midway analysis in April 1999, and a final analysis in February 2000 – to analyze the benefits and results of the paper-less office till date.

The first check conducted in September 1998 was several weeks after the commencement of the paper-less office effort. The purpose of this analysis was to review the commitment and involvement of the various parties involved (the Project; Modern Continental the Contractor; and MIT) in the ongoing effort and to define a roadmap for the development of the paper-less office in the coming months. At this stage Modern Continental the contractor, was not fully committed to this effort, as senior management at Modern Continental perceived that the paper-less office will have access to confidential internal documents, as well as, most significant benefits of paper-less office effort would be in

favor of the Project and not towards them. On the other hand, the paper-less office was receiving great support from senior management at the Project, as well as, the IT and construction departments of the Project. In the coming months, Modern Continental began to view their involvement in the paper-less office effort as a learning experience that would enable them to take a leading role in similar implementations in future projects and hence increase their competitiveness in the global construction market. This change of perspective motivated Modern Continental to play a pivotal role in the implementation of the paper-less office. At this early stage of the implementation, it was noticeable how organizational issues started playing and would continue to play a pivotal role on the ability for the test office implementation to reach its full potential.

The second check, conducted in April 1999, was in essence a "reality-check" on the progress of the paper-less office till that date. This was a stage at which a framework for implementing (based on meetings between the contract C19E1, Modern Continental and MIT) the paper-less office had been identified and prototypes based on this framework were being implemented. In the months preceding this survey, the paper-less office had, with research support from MIT, identified the requirements for developing a paper-less office. During that period the existing infrastructure was analyzed, new technologies were identified and a framework based on the models for secure communication and secure information management, as discussed in this thesis, had been created. At this stage a survey was conducted with the engineers in the contract to get feedback on the impact of the ongoing implementation and their views about its perceived advantages. This was based on the existing automation within the Project, which was being extended to the contractors in the form of the framework that the paper-less office was implementing. The general response was that automation offered tangible benefits in the areas of document preparation, information retrieval and information sharing. The engineers felt that every project process should be automated (and not just a few), but realized that the complexities of each process varied and hence needed a different amount of planning and co-ordination.

At that stage, the biggest challenge in creating an information management framework for the paper-less office was in dealing with the issues of security and reliability that has been the focus of this thesis. This was a prime concern to the Project as well as the contractor, Modern Continental, as they would be sharing a common information infrastructure. The survey reflected that the engineers were very concerned about the security and reliability of the on-going automation and partnering. One of the responses in the survey that reflected the importance of security and network reliability in the ongoing automation process was that *"The system (that is being implemented) is only as reliable the network it's on."* The engineers did acknowledge the advantage of automation during claims and this is reflected in one of the responses as *"because information on claims and changes is available more readily, they are being processed more efficiently and this has helped support partnering on the contract."* Another survey respondent complemented this by saying that *"Claims & Changes file information (Letters, Drawings, FCNs. Modifications etc.) are now very accessible and much easier to retrieve than "hard-copies". This has increased the efficiency of Claims processing."* Most engineers also acknowledged that the paper-less office saved time and effort in the preparation of documents in the form of responses such as *"Important letters that sometimes took a day for the addressee to receive, now takes seconds to receive."* For example, an analysis of the turnaround time for Request for Information (RFI) documents over a period of months showed considerable reduction in time due to the automation process. The engineers also realized that in order to reap the benefits of automation in claims, electronic transactions need to be secure and binding as explained in this thesis.

Though security and reliability was a major issue, the other big challenge, as in any large-scale system integration effort, was the issue of in-compatibility between existing infrastructure within the project and that of the contractor. A mutual agreement was reached upon how best to use the existing infrastructure and reduce new investments in areas that would not offer new functionality. For example, the Project didn't want to make a new investment in document management systems as they had already invested in KeyFile [Keyfile Corporation, 2000] to provide this functionality, while the contractor

had made an investment in Microsoft Exchange Server [Microsoft Corporation, 2000] to serve as a messaging server and document repository.

At this stage, the paper-less office's participants felt they had identified most of the important steps needed to be taken for the creation of the office, like an implementation based on the framework for secure and binding transactions developed by MIT and a system integration plan for the information systems in the Project and the contractor. This check proved that the project's senior management and IT task force were optimistic about the prospects of the test-office's paper-less implementation based on the progress till that date. Hence, it was decided to completely automate most of the important work process in the contract like the Request for Information (RFI) and Pending Change Order (PCN) to name a few, some of which had already been implemented in months leading to this check.

About nine months later, in February 2000 a final analysis of the paper-less office implementation was performed and the IT task force presented a report to the Deputy Director of the Project. Compared to the midway analysis, the final analysis was less optimistic about the success of the paper-less office implementation. Since the interim period between the two analyses was the final implementation period of the paper-less office, a lot of implementation specific problems, which were overlooked, surfaced. A lack of adequately trained staff to fulfill the needs of the implementation was a major concern and hence it affected the implementation of the paper-less office in the envisioned scope. This problem was further aggravated by the fact that the simple workflow diagrams in the paper-based scenario when translated to the electronic scenario were tough to implement, both organizationally and technically. The lack of full appreciation for the amount of programming/development at the design stage was also clearly visible during implementation. The initial perception that off-the-shelf software solutions could be integrated into the paper less implementation was not as easy as envisioned. Apart from these technology-related problems there were also organizational problems like resistance to change, staff attitude and commitment, unreasonable enhancement of scope and staff reduction due to turnover.

The paper-less office was bringing a definite change in the way the staff in the contract was doing day-to-day business and though this received a lot of support during the pre-implementation and early phase, it received resistance during the final implementation phase. The inconvenience due to the time spent in getting familiar with the technology to perform simple tasks was a frustrating experience for some of the staff. This was further augmented by the lack of enough IT support staff to assist the users in the transition from paper-based transactions to electronic transactions.

Based on these observations, the IT task force came to the conclusion (which formed part of its recommendation to senior management) that the paper-less office *"was too idealistic"* in terms of setting its vision. It was realized that the task of *"seamlessly melding the existing IT operations of the Project (in contract C19E1) with discrete operations of the general contractor (Modern Continental) was more than the under-staffed IT team in the project could achieve in the given period of time."* Thus, the implementation showcased the need for organizational change, support and management in order to effectively re-engineer business processes in the A/E/C industry.

In-spite of these problems the paper-less office implementation had a number of benefits. As of February 2000, the implementation of the paper-less office in Contract C19E1 at the Central Artery Project had produced a number of benefits. The implementation on this particular contract had helped create methodologies for automation of important project's processes like Requests for Information (RFIs), Pending Change Notices (PCNs), Deficiency Reports (DRs). An automated workflow methodology for each of the processes had also been created for use in the project. Along with a set of automation methodologies the test implementation had created a set of trained personnel to successfully extend the paper-less office to other contracts in the project. In terms of using new technology, digital IDs and digitized signatures were used to electronically transmit transaction information but the full implementation of a transaction management system based on this technology was hampered due to some of the organizational problems discussed in this section. Currently three other contracts in the Project are

implementing paper-less offices. However due to the steep learning curve, as gauged from the test office implementation, the approach has been reduced in scope in these contracts. In these new contracts, due to lessons learnt from the test office implementation, special attention would be given to organizational issues such as training, personnel capability and motivation. In addition, the success of the test office had not only benefited the project but also the contractor Modern Continental Inc. Differences in commitments and priorities between the contractor, Modern Continental, and the project affected motivation in the early stages of implementation but the perceived benefits helped overcome differences and led to a moderately successful implementation. Modern Continental is now in a position to take a lead role in similar implementations in other projects, based on the experience gained at the Central Artery Project.

Though the grand vision of the paper-less office has not yet been achieved, the test office has provided a number of benefits as discussed in this section and it is based on these benefits that senior management in the project has decided to implement paper-less offices in three other contracts, though with lower scope. In summary, one of the most important lessons learnt from the paper-less office experience was that though there are numerous technology related problems during implementation, progress is eventually hampered primarily due to organizational issues like change, training, personnel commitment and motivation. Nevertheless, in the next section some of the technology-related deployment issues of the framework for secure and binding electronic transactions developed in this thesis, are discussed.

7.5 Deployment Issues

The framework for secure and binding electronic transactions described in this thesis possesses a fair degree of scalability allowing it not only to be, ported to different kinds of projects with ease, but also to be compatible with technologies of the future. The web-based architecture used for this framework provides a distinct advantage over the traditional client-server architecture with respect to the deployment of this framework in

large-scale engineering projects. In a large-scale engineering project the format of documents change with time and this would require changes to the application. If the traditional client-server model were followed, the new version of the client application needs to be redistributed to every user and this would be a challenge in large-scale projects where the users could be globally distributed. On the contrary, in the case of web-based applications, new versions, released on the server, are immediately accessible to the user.

In order to achieve scalability, the architecture of the proposed framework is completely component-based (see Figure 7-3). Technology changes in the future or project-specific requirements may warrant the addition or removal of components in the present architecture. The component-based design of the architecture would not only allow for such changes to be made with minimum rework but also be re-deployed with ease. The framework also supports components like digitized signatures that are scalable to paper-based documents. This not only eases the transition from paper-based transactions to electronic transactions, but also facilitates the creation of legally binding paper copies of the electronic transactions.

The framework presented in this thesis also possesses ample redundancy in its architecture to minimize the occurrence of failure, which would be unacceptable in this critical application. There are multiple communication channels (see Section 7.2) in the architecture in order to prevent disruption in information flow in case a particular communication channel fails. There is also a provision for multiple security mechanisms like fingerprint verification, face verification and signature verification. In the event of a particular security database being inaccessible or off-line, verification can be done using a different biometric mechanism without providing any disruption in service to the users of the system. Having discussed some of the technology-related deployment issues of the framework for secure and binding electronic transactions, in the next section the future direction of this research effort is discussed.

7.6 Future Research

Future research work in this area is two fold in nature; on one hand technology related issues related to the deployment of the framework discussed in this thesis need to be researched, while on the other hand, organizational challenges and issues related to implementing IT strategies in large-scale A/E/C projects need to be researched.

The technology issues which need to be researched include challenges in implementing and deploying distributed web-centric project management systems in large-scale A/E/C projects (such as the CA/T Project) like feasibility, performance, fault-tolerance and reliability. Deployment of the framework, developed in this thesis, to a large user-base, as in the case of very large projects like the Central Artery Tunnel Project, would require the use of multiple servers, for load-balancing, to achieve high performance. There is a plan to simulate at-least couple of thousand concurrent "hits" to the system in order to study the performance and behavior of the system under high load conditions. The simulation would give results on server response-time and reliability which would help make an estimate on the number of servers required to maintain optimum performance levels in-spite a large user-base. It is also planned to create metrics for measuring Quality of Service (QOS) of these project management services within a large-scale A/E/C project. As an extension to the model for information management, there is also a need to address the critical issue of storing electronic information over long periods of time, as required by most large-scale A/E/C projects. Public projects like the Central Artery Tunnel Project typically need to store some project information for at least 99 years. This is also required to achieve one of the broad visions of this framework, that of scalability over time. With document and data storage technologies changing rapidly with time, this would be a major challenge.

As discussed earlier (and as witnessed in the test office implementation at the Central Artery Project), though technology is vital, it is organizational issues, that, to a large extent determine the success or failure, of large scale IT implementations in A/E/C projects. Thus, apart from technology related issues, organizational issues like the ability

to effectively manage change, employee morale and commitment in large-scale A/E/C projects during IT-based business process re-engineering of the scale that was witnessed in the Central Artery Project, during the implementation of the paper-less office are also being currently researched [Peña-Mora, Vadhavkar et al, 1999]. This effort would also include determining metrics for measuring Return on Investment (ROI) on Information Technology (IT), in order to justify the large investments made by organizations involved in large-scale A/E/C projects.

7.7 Summary

This chapter discussed the application of the framework developed in the previous chapters on a test case - the $13.6 Billion Central Artery Tunnel (CA/T) Project in Boston. The framework was developed to conduct secure and legally binding business-to-business transactions within a specific industry, namely the A/E/C industry. Having developed a framework for a specific industry the next step was to work towards developing a generic framework for conducting secure and binding B2B, B2C, G2B and G2C transactions through the creation of an e-notary service. While the following chapters (8–10) discuss the development of the e-notary service, the next chapter discusses the scope of the e-notary and the influence of the first phase of this research effort in its development.

Chapter 8

Towards a Generic Framework for Conducting Secure and Legally Binding Electronic Transactions

The last six chapters of this thesis - constituting the first phase of this thesis – discussed the development of a framework for conducting secure and legally binding transactions in a specific industry segment, namely the A/E/C industry. Having developed a framework that has the potential to achieve a major replacement of paper-based transactions with secure electronic transactions, in the A/E/C industry, there was ample potential, to use the components of this framework and the findings of the research in the first phase to develop a generic framework for conducting secure and legally binding electronic transactions.

8.1 A Generic Framework for Conducing Secure and Legally Binding Electronic Transactions

The A/E/C industry, because of its structure and organization, size, geographically distributed nature and reluctance to achieve large-scale replacement of paper-based transactions, proved to be a perfect test-bed for developing a framework for secure and legally binding electronic transactions, which would achieve a major transition from paper-based transactions to electronic transactions. The initial period, of the first phase of this research effort, was used to study the security concerns [see Chapter 3] in conducting electronic transactions in large-scale A/E/C projects. These concerns, to a large extent, are similar to security concerns in other industries, in conducting electronic transactions, and hence the framework developed for large-scale A/E/C projects could be extended across industry segments. In essence, the A/E/C specific implementation, in the first phase of this research effort, not only provided very valuable insight into some of the most important concerns in conducting electronic transactions today, but also highlighted the technology components required to conduct secure and legally binding transactions over the Internet, through the creation of models for secure communication and secure information management [see Figure 8-1].

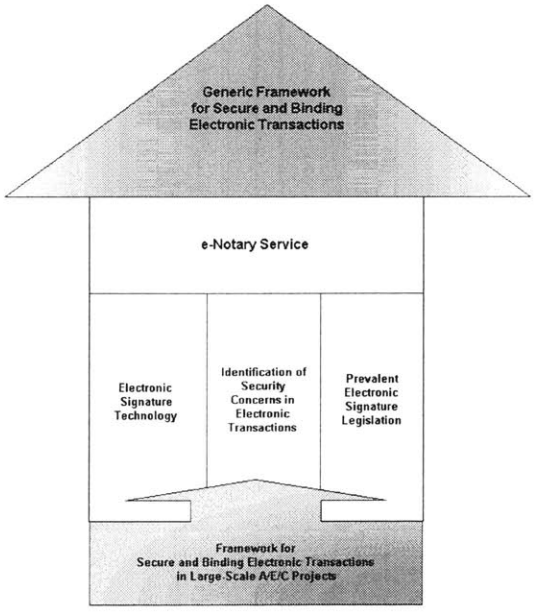


Figure 8-1: Towards a Generic Framework for Secure and Binding Electronic transactions

It was also useful in reviewing the e-commerce (electronic signature) legislation which influences, to a large extent, the legally abidingness of electronic transactions. In the next two chapters – the second phase of this research effort – a generic framework for conducting secure and legally binding electronic transactions is developed through the vision of a next generation e-Notary service.

8.2 Summary:

Having motivated the need for a generic framework for secure and binding electronic transactions in this chapter, the next two chapters discuss the development of an e-Notary service that addresses this critical need. While the next chapter discusses the vision for an e-Notary service and its functional architecture, Chapter 10 discusses the system architecture for a working prototype and its application on a test case.

Chapter 9

An e-Notary Service

9.1 What is an e-Notary?

An e-Notary is envisioned to be a service that facilitates secure and legally binding electronic transactions over the Internet (see Figure 9-1). It would provide value to e-commerce or other Internet-based transaction services, consumers, as well as third party security service vendors (through strategic partnerships) as follows:

E-commerce/Internet-based Services:

- It would allow E-commerce/Internet-based services (offered in the industry, as well as, the government) to implement their security policy through the e-Notary service. This would allow them to focus on their core business while the e-Notary provided them with the required services to conduct secure, legally binding electronic transactions with other businesses, the government or consumers.

- Though the e-Notary service provides the security services, e-commerce/Internet-based services would have the flexibility to customize the service according to their needs. Though, the e-Notary service would offer ready to use security templates, it would also offer the flexibility to build a configuration from scratch.

- The e-Notary service would serve as a trusted third-party that provides the electronic evidence for the occurrence of the electronic transaction in the event of legal disputes.

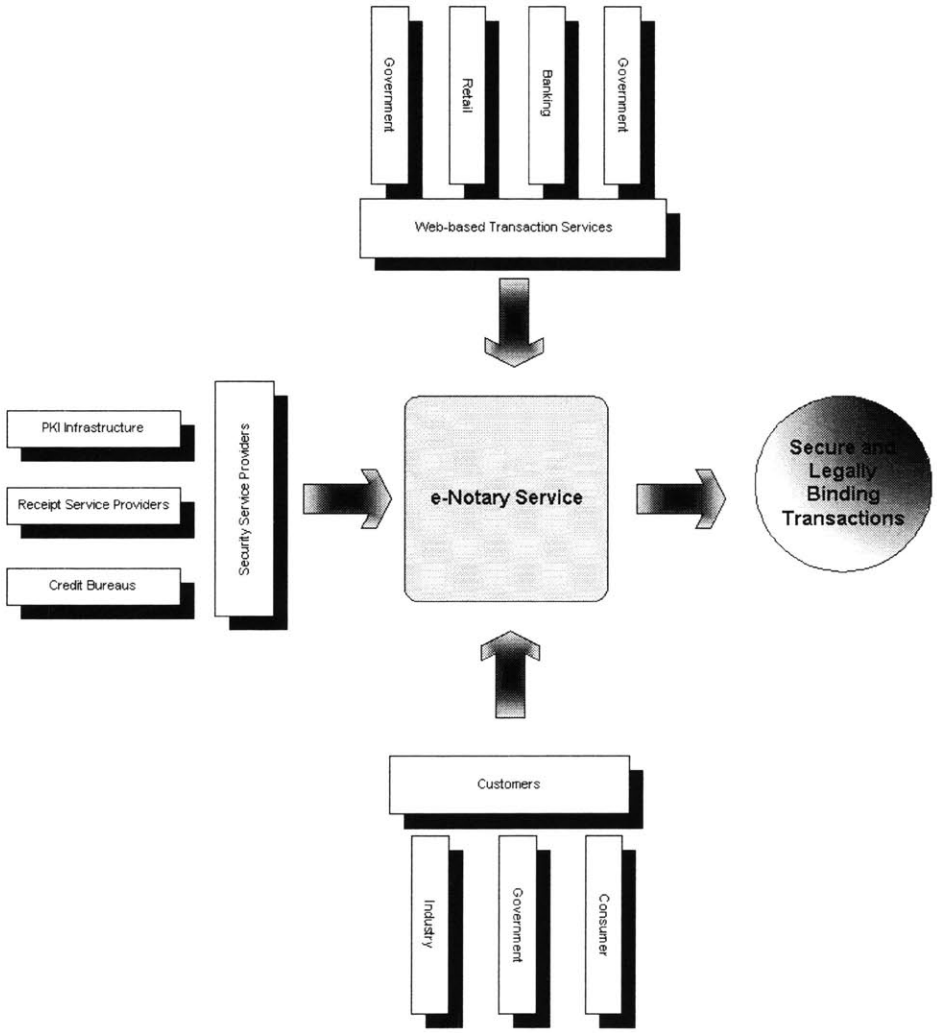


Figure 9-1: Vision for an e-Notary Service

Customers:

- The e-Notary Service would offer a Smart Receipt to customers for every transaction that he/she participates in. The Smart Receipts would have an audit trail for the entire transaction that would legally bind the e-commerce company, as well as, the customer to the transaction after it has been committed. In essence the audit trail would provide electronic evidence (e-evidence) for the occurrence of the transaction and neither the client nor the service could repudiate their participation in it.

- The e-Notary service would provide clients with a Smart Receipt Wallet that would organize and store all the Smart Receipts of the consumer. The Smart Receipt Wallet could be used to check the integrity of the transaction, through the e-Notary service, at any time.

- It would allow customers to participate in transactions using a range of security mechanisms – biometric, infometric and PKI-based- like digital signatures, handwritten signatures, passwords, voice recognition that are acceptable to the e-commerce/ Internet-based service, as well as, are legally binding in the state where the jurisdiction for the transaction lies.

Third Party Security Service Providers:

- Through strategic tie-ups the e-Notary service would offer security service providers like Certificate Authorities access to its customers.

9.2 Functional Architecture

Based on the security concerns for conducting electronic transactions, as defined in Chapter 3, and a study of paper-based transactions in industry and government the functional architecture (see Figure 9-2) of the e-Notary service was determined.

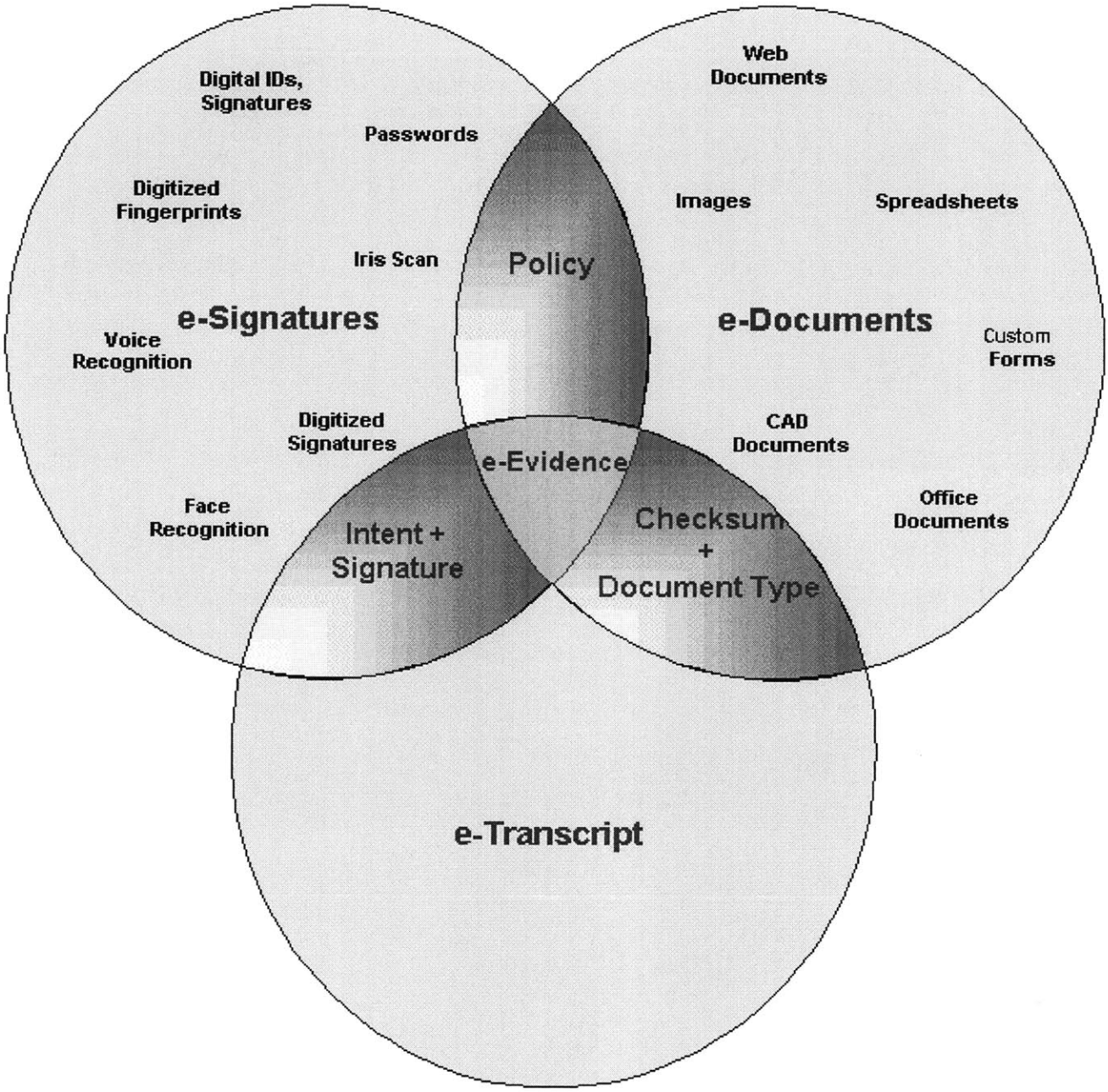


Figure 9-2: Functional Architecture of an e-Notary Service

9.2.1 Identification Mechanisms (e-Signature)

As discussed in Chapter 3, precise identification is one of the most important requirements for conducting secure and legally binding electronic transactions. Precise identification is required to prevent non-repudiation by transaction participants, as well as, to provide secure access-control. Electronic evidence (e-evidence) recorded by the e-Notary service during a transaction would vary according the prevalent e-commerce laws [Perkins Coie LLP, 2000] in the state or country where the jurisdiction for the transaction lies. Thus, the e-Notary needs to support a range of identification of mechanisms (see Figure 9-3) ranging from biometrics, infometrics to PKI based identification.

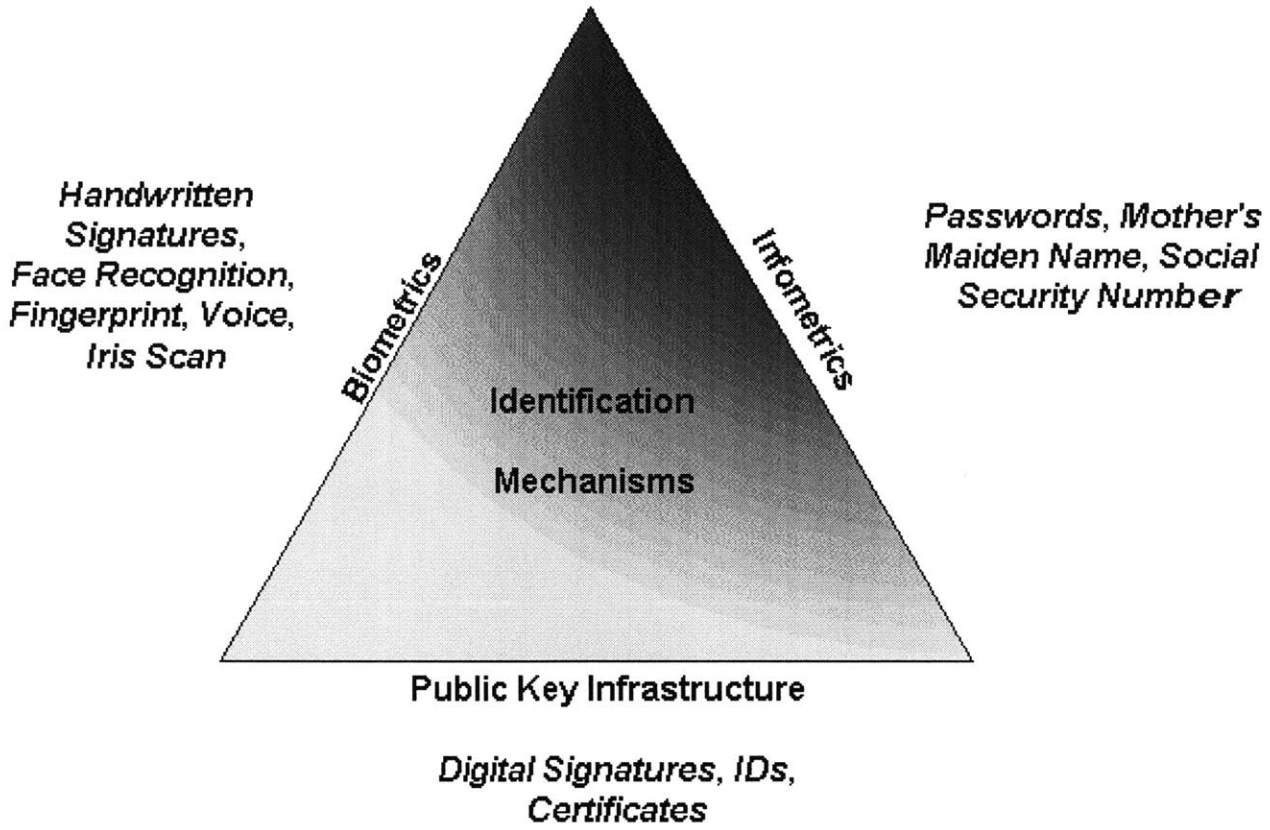


Figure 9-3: Identification Mechanisms

The identification mechanisms (see Figure 9-3) vary from one another in the security they offer and the cost of implementation (see Figure 9-4).

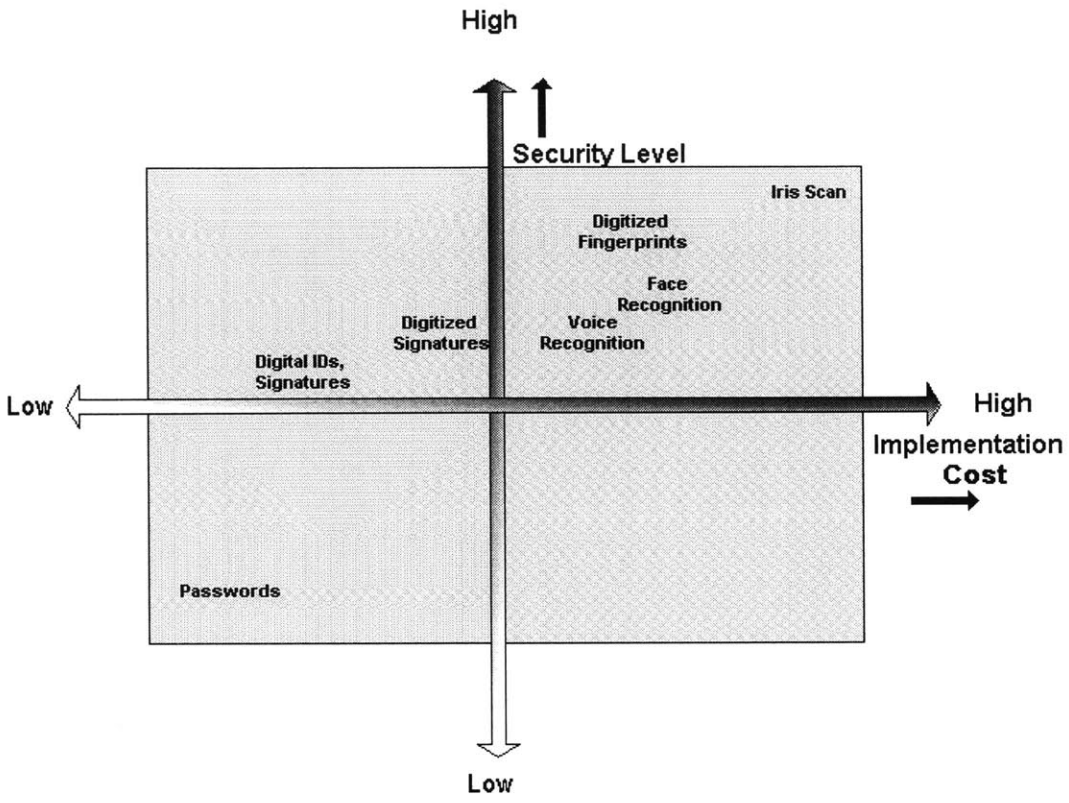


Figure 9-4: Identification Mechanisms' Cost – Security Matrix

9.2.2 Electronic Documents (e-Document)

Transaction documents could range from web-documents (see Figure 9-2) in Java [Javasoft, 2000], XML [XML.org, 2000] to office documents in Word [Microsoft, 2000] PS [Adobe, 2000], Adobe [Adobe, 2000] to CAD Documents to name a few. Thus, the e-Notary service should allow for a wide range of document formats for use in electronic transactions.

9.2.3 Security Policy

The e-Notary service needs to provide web-based transaction service providers with the flexibility to implement their own security policy. Security policy could be based on document types, signature mechanisms, transaction types, and relevant signature laws to

name a few. Security policy determines (see Figure 9-2) the relation between a signature mechanism and a document type.

9.2.4 Electronic Evidence for Transaction (e-Evidence)

The primary purpose of the e-Notary service is to provide legally valid electronic evidence (e-evidence) for the occurrence of electronic transactions. The e-Notary service needs to provide e-evidence to all the transaction participants, as well as, securely store the evidence locally, for future verification by the customer or the transaction service provider. The e-evidence would include a transcript of the transaction in a manner that would legally prove the occurrence of the transaction and its contents, based on the electronic laws prevalent in the location, where the jurisdiction for the transaction lies. In essence the e-evidence needs to provide the *"Who, Why, What, Where, When"* for an electronic transaction (see Figure 9-5). The following components constitute the e-evidence:

- **Signature:** As discussed in Section 9.2.1, a legally valid e-signature that could range from a password, to a voice recording, to his/her digitized handwritten signature.

- **Intent of Approval:** An intent of approval, collected as part of the transaction transcript, that could range from a sequence of the customer's mouse clicks during the transaction, to recording his/her voice stream stating his/her approval of the transaction.

- **Policy:** The security policy for the transaction service provider at the time of the transaction.

- **Document Type:** The format of the document that was approved.

- **Checksum:** A unique digital "fingerprint"(see Section 6.2) of the information in the document that was approved. It secures the content of the transaction that occurred to prevent any of the transaction participants from altering it to their benefit.

- **Time Stamp:** A digital timestamp of the transaction.

- **Machine Number/Network Address:** To identify the location of the transaction participant to the extent possible.

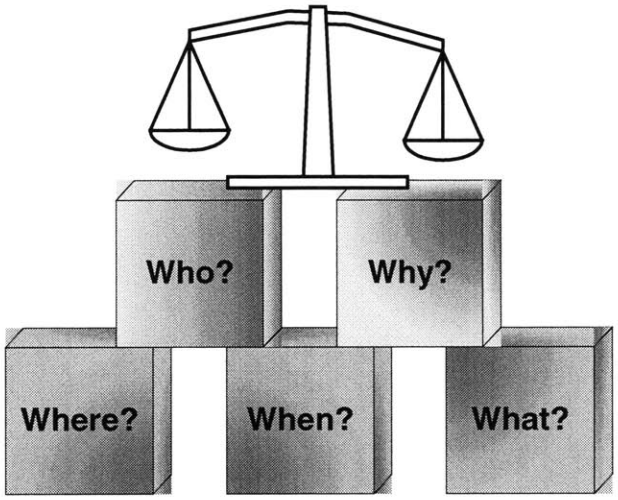


Figure 9-5: *"Who, Why, What, Where, When"* – The building blocks of legal e-evidence

9.2.5 Secure Data Exchange

Since most electronic transactions occur over public networks like the Internet transaction data and related security information needs to be secured from tampering and unauthorized viewing. In order to achieve secure communication, the data transmitted between the transaction participants and the e-Notary service needs to be authenticated and encrypted (see Section for 5.1 & 5.2).

9.2.6 Scalability

With rapidly changing data storage technologies and security mechanisms, the architecture of the e-Notary service needs to be scalable to adapt to the technologies of the future.

9.3 Summary

This chapter discussed the vision for an e-Notary service and its functional components. The e-Notary service would serve to fulfill the vision for a generic web-centric framework for conducting secure and legally binding electronic transactions. The next chapter discusses the system architecture of the prototype version of an e-Notary service and its application on a test case namely, a web-based stock brokerage.

Chapter 10

e-Notary: System Components and Architecture

Having discussed the vision and functional architecture of an e-Notary service in the last chapter, this chapter describes the components and architecture of a prototype implementation of an e-Notary. The prototype design offers only a subset of the functionality described in the last Chapter (see Figure 9-2), but offers the proof-of-concept of an e-Notary service, and valuable feedback that would be useful for developing the next generation e-Notary.

10.1 System Components

The functional architecture of the e-Service Provider has been implemented in the form of a web-based system with the following components (see Figure 10-1):

10.1.1 Transaction Database

The transaction database is implemented by the transaction service provider to provide its business services. It is independent of the transaction security policy that is implemented by the organization that is in turn outsourced to the e-Notary.

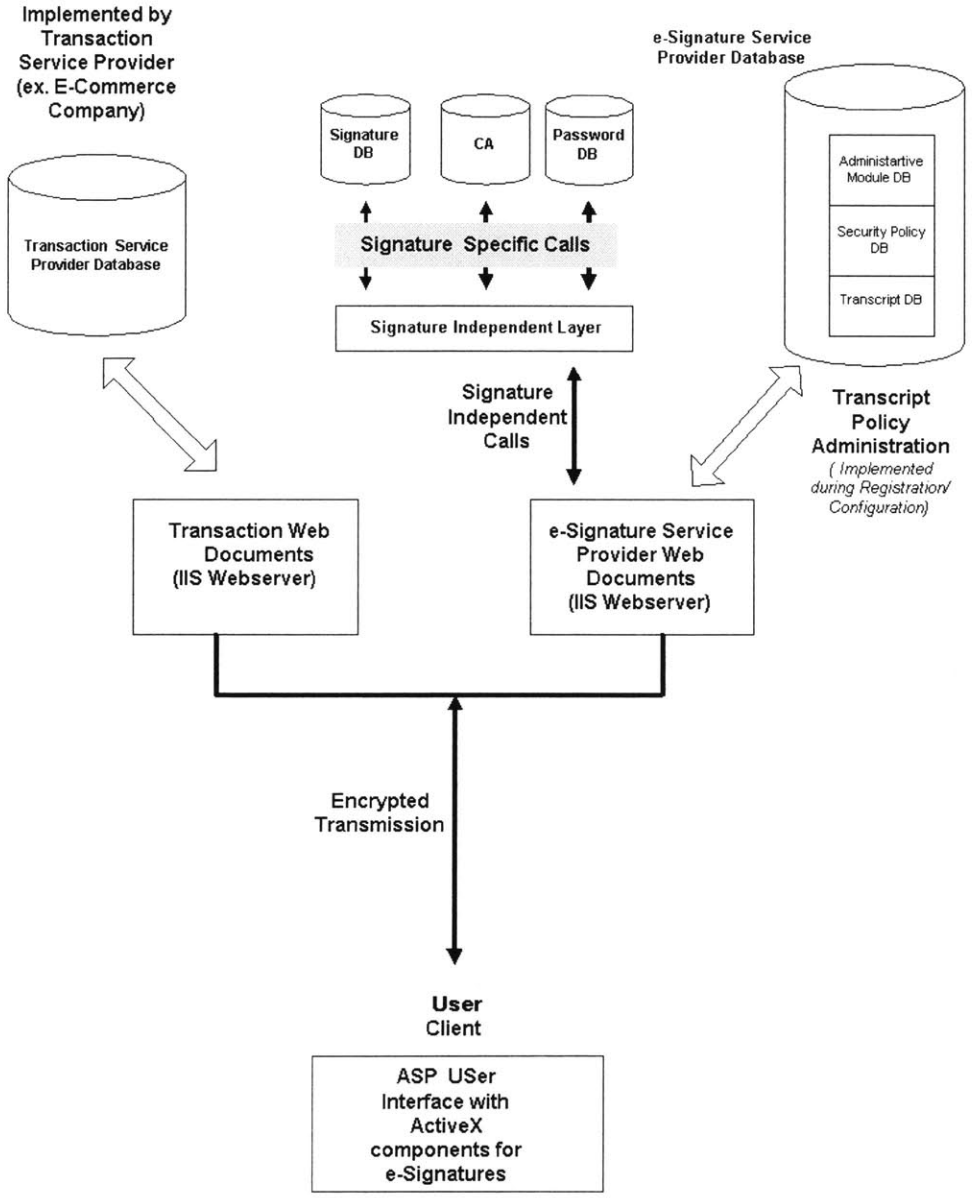


Figure 10-1: e-Notary System Architecture

10.1.2 e-Notary Database

This database is used to implement the transaction security policy of the e-Notary service and is independent of the transaction database. This database is configured by the transaction service provider, at the time the latter registers with the e-Notary to avail its security services.

10.1.3 Transaction Server

The Transaction Server contains all the transaction service related web documents as implemented by the Transaction Service Provider. It redirects the users to the e-Notary service at the point the customer is ready to commit the transaction. In the prototype, the web documents use Active Server Pages (ASP) [Microsoft, 2000] technology hence the Microsoft Internet Information Server (IIS) [Microsoft, 2000] is used as the transaction web-server.

10.1.4 e-Notary Server

The e-Notary Server consists of web-documents that verify authenticity and commit legally binding electronic transactions to the e-Notary database, as well as, the transaction database. It also provides the interface for users to register their security information for use in transaction.

10.1.5 e-Signature Interface

The e-Signature interface allows e-Notary to query e-signature databases to verify user authenticity. It provides signature independent services to e-Notary's web documents accessing digitized signature databases, Certificate Authorities and Password databases.

10.1.6 Web Client

The browser-based user client allows users to participate in secure, legally binding electronic transactions. It offers complete transparency to the user who is unaware that the transaction is being implemented by two entities (Transaction Service Provider and e-Notary). The communication between the client and the servers is encrypted to provide secure transfer of transaction and security data.

10.2 Database Design

The system architecture (see Figure 10-1) consists of two distinct databases namely the Transaction Service Database and the e-Notary Database. While the transaction database is implemented by the transaction service provider for the implementation of its business processes, the e-Notary Database is used solely for facilitating secure and legally binding electronic transactions. The e-Notary database is used to provide administration of users, security policies and transaction transcripts.

10.2.1 User Administration

The user administration database, used to implement the administrative interface for the e-Notary, also acts as an interface to the transaction management system (Transaction Database) implemented by Transaction Service Provider.

10.2.2 Security Policy

The security policy database is used to determine/implement the security policy of the organization with respect to a transaction, user, document type and signature mechanism. Ideally, the criteria for using a particular policy would depend on the one or more of the following –

a) Location from where a particular user is participating in a transaction – Listed IP or Unlisted IP?
b) Country/State where the jurisdiction for the transaction lies?
c) Type of Transaction (Ex: What is the person buying) - The e-commerce company could use different kinds of policies for different types of transactions.
d) Mode of Payment
e) Value of Transaction – Range

10.2.3 Transaction Transcript

The transcript database is used to create a legally acceptable transcript or audit trail for the transaction that has been administered by the e-Notary service. The transcript database records the intent of the transaction participant, document type, e-signatures and transaction checksum.

10.3 Smart Receipt

The Smart Receipt (see Figure 10-2) is an electronic receipt generated by the e-Notary service for every completed transaction. After the user commits a transaction, the e-Notary dynamically creates a Smart Receipt that contains a summary of the transaction (as specified by the transaction service provider) and legally binding information relating the user to the transaction. This receipt can be stored electronically in the smart wallet or printed to create a paper copy.

10.3.1 Why is the receipt smart?

- It is generated dynamically for a particular type of transaction and user, as defined in the transaction service provider's security policy during its registration with the e-Notary service.

- It legally binds a person to a transaction by providing electronic evidence (e-evidence) for the transaction.

- It can be stored in electronic form securely by the user locally.

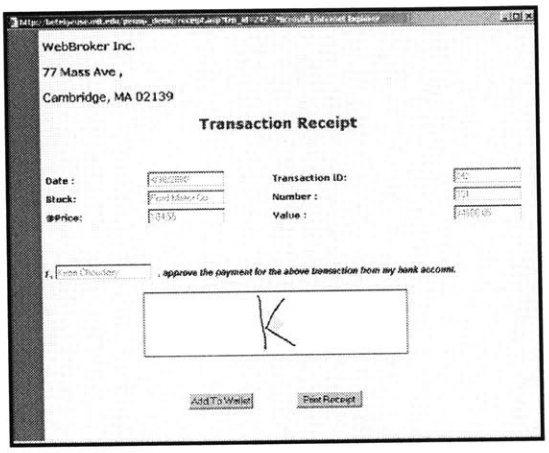


Figure 10-2: Smart Receipt

10.4 Smart Receipt Wallet

The Smart Receipt Wallet (see Figure 10-3) is an application that organizes/stores Smart Receipts created by the e-Notary. It can be developed as a desktop application or browser based application. It is used to verify the integrity of the digital evidence in the Smart Receipts.

10.4.1 Why is the receipt wallet smart?

- It can verify the integrity of the receipt as well as the transaction
- It organizes /secures receipts

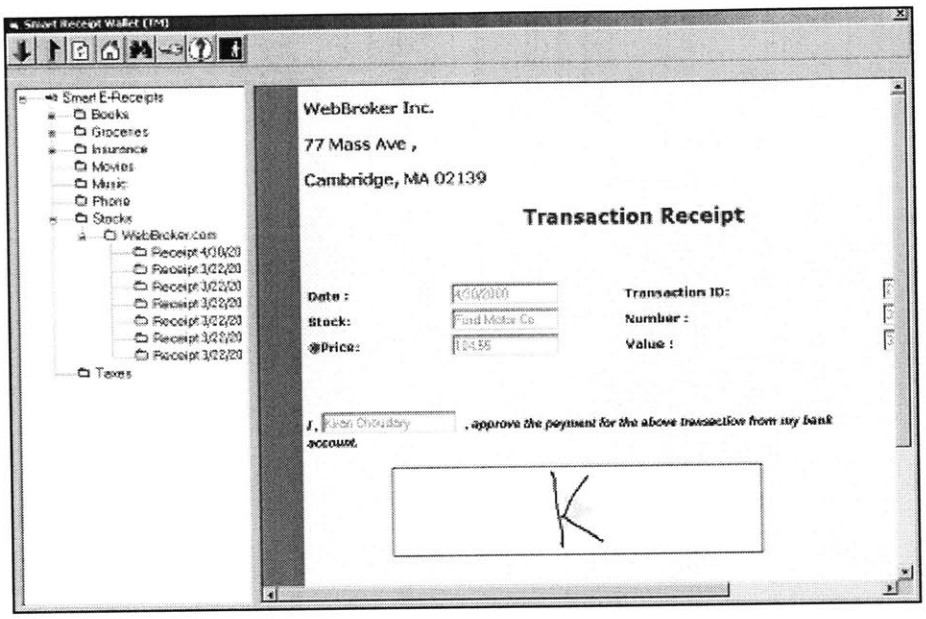


Figure 10-3: Smart Receipt Wallet

10.5 Pilot Case: A Web-based Stock Broker

A web-based stockbroker scenario was used as a pilot case for implementing the prototype version of the e-Notary service. The web-based stockbroker known as *"Web-Broker.com"*, a simple service that allows consumers to buy stocks over the Internet, uses the services of an e-Notary to conduct secure and binding electronic transactions. The various components of this pilot case implementation are as follows:

10.5.1 User Registration Procedure

The user registration procedure (see Figure 10-4) at *Web-Broker.com* includes registration with the e-commerce company namely, *Web-broker.com,* as well as the e-Notary service.

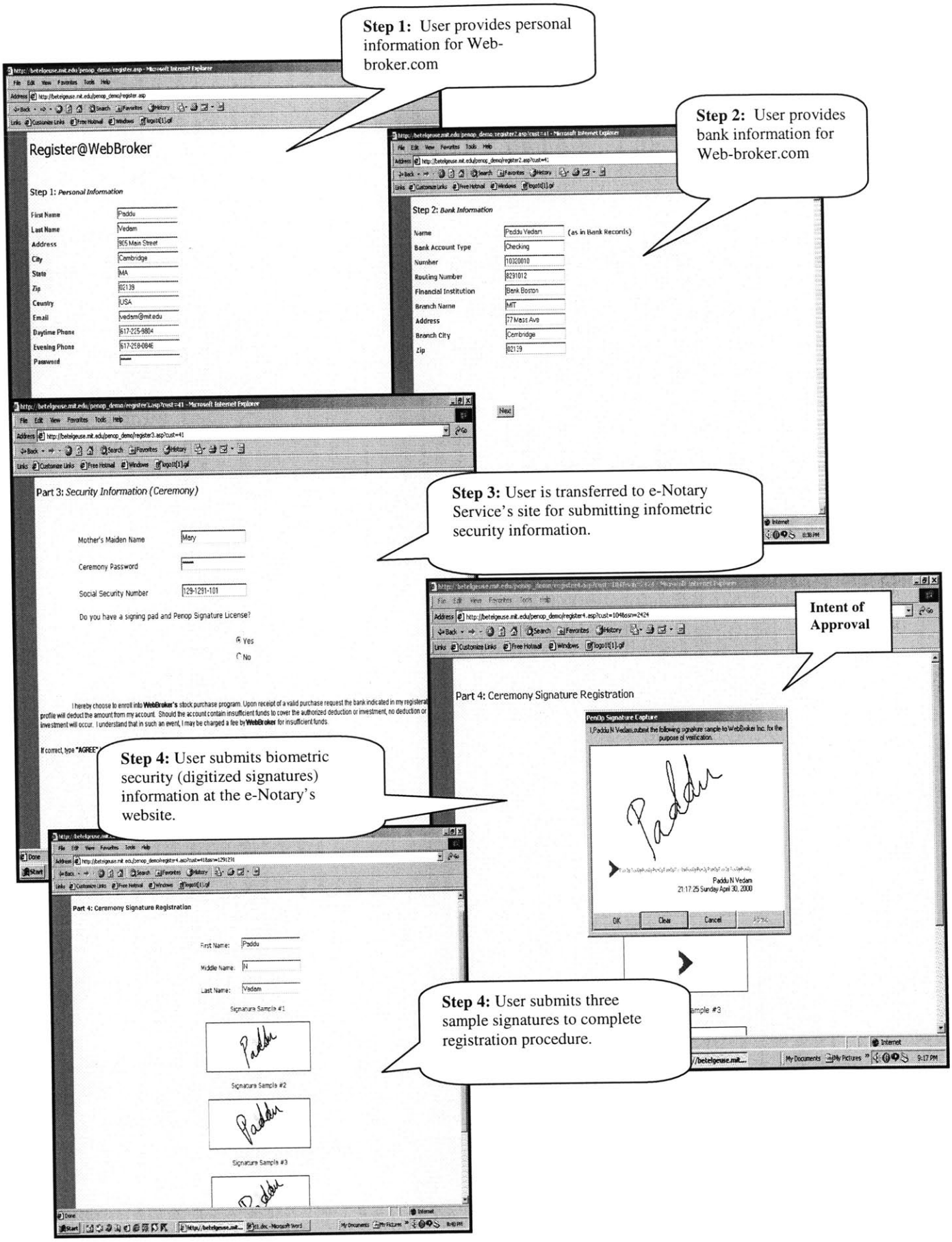


Figure 10-4: User Registration Procedure

10.5.2 A Simple Secure and Legally Binding Transaction

Once the user has registered at *Web-broker.com* he/she can participate in a secure and legally binding online stock purchase transaction (see Figure 10-5).

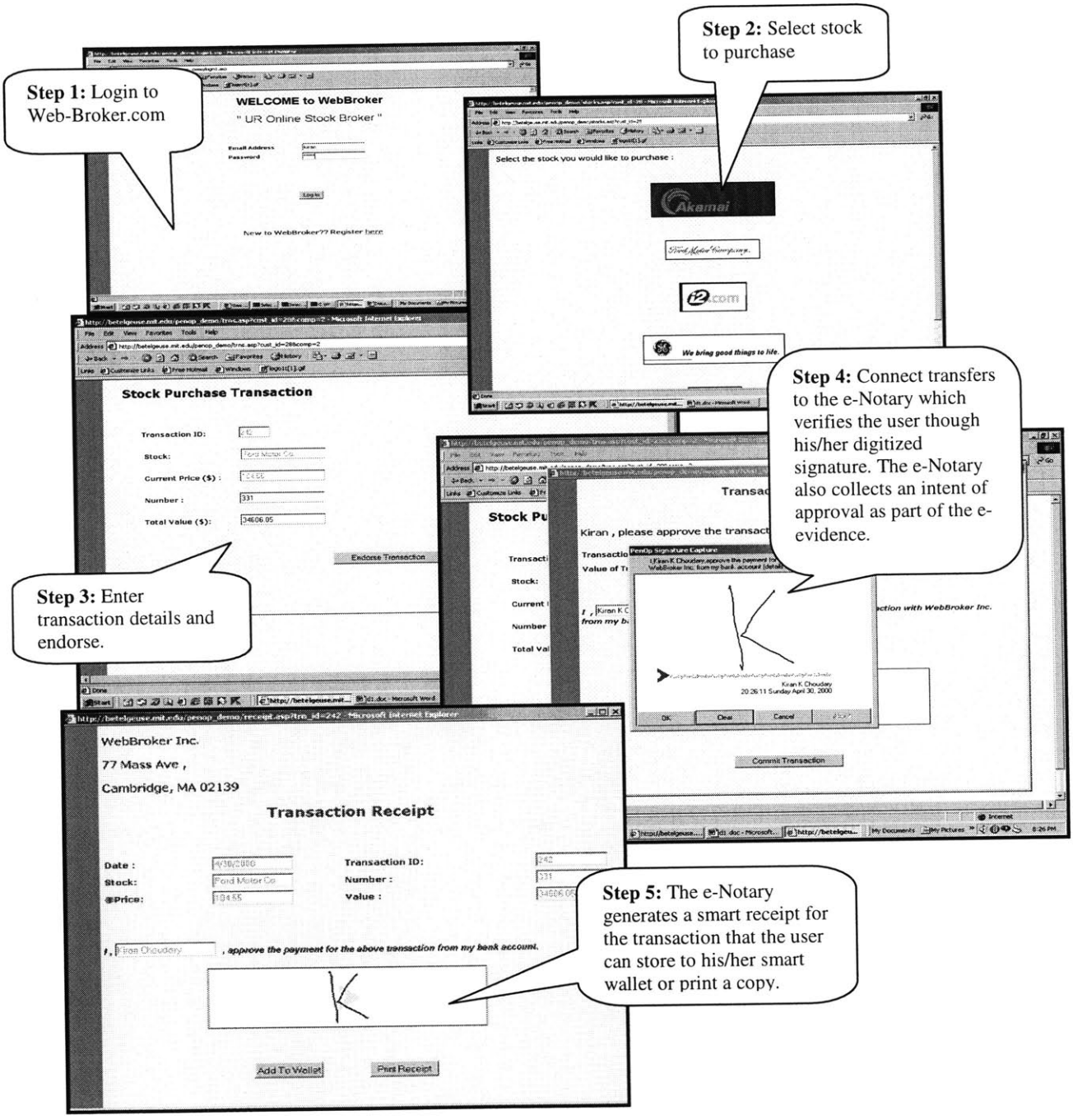


Figure 10-5: A Simple Secure and Legally Binding Transaction

10.5.3 Smart Receipt

Once the smart receipt has been generated containing the electronic evidence for the electronic transaction the user can save it to his/her smart wallet (see Figure 10-6).

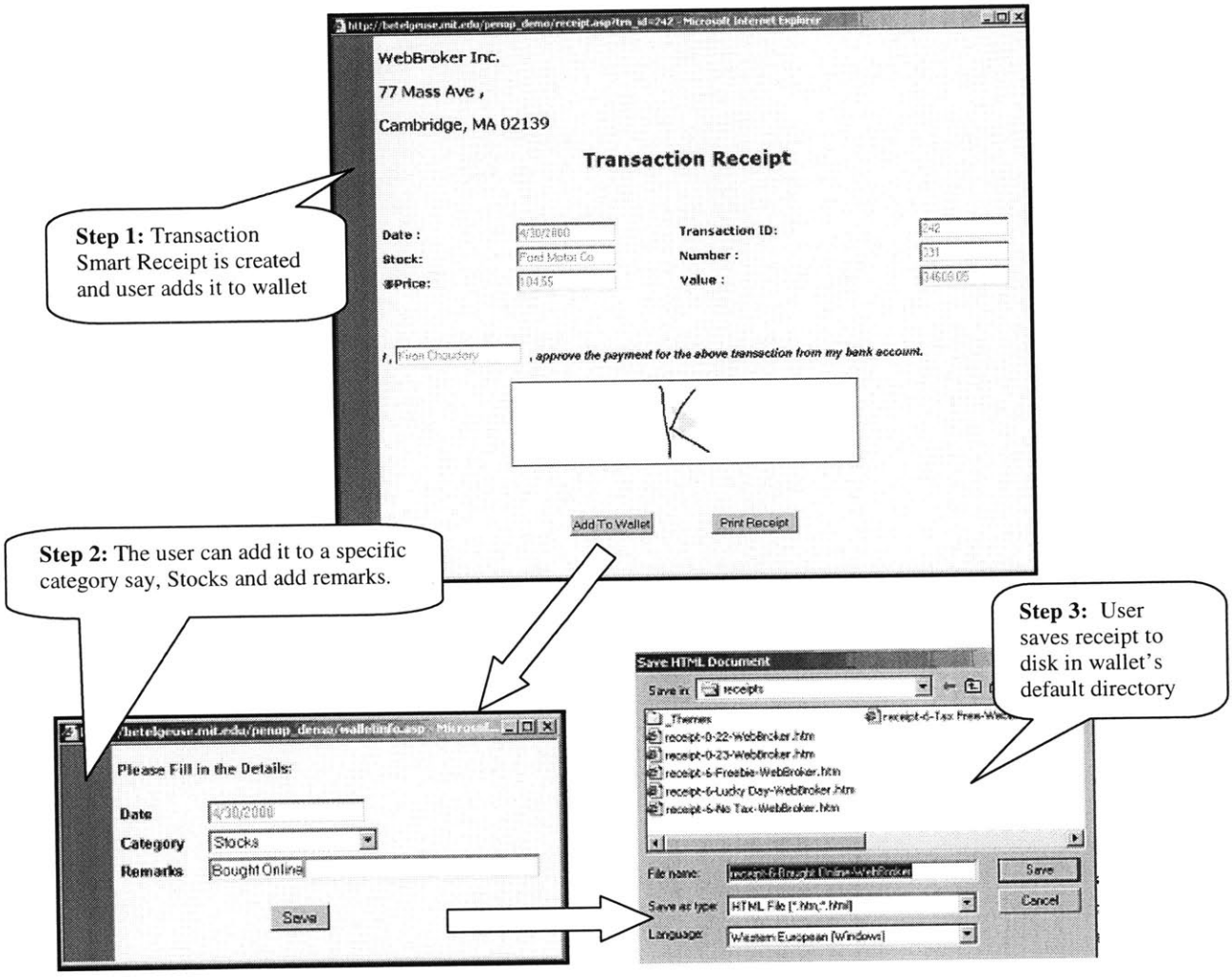


Figure 10-6: Adding a Smart-Receipt to the Smart Wallet

10.5.4 Smart Receipt Wallet

Once the receipt has been added to the Smart Receipt Wallet it's integrity can be verified by comparing the checksum of the receipt in the wallet to the checksum of the transaction at the e-Notary Service (see Figure 10-7)

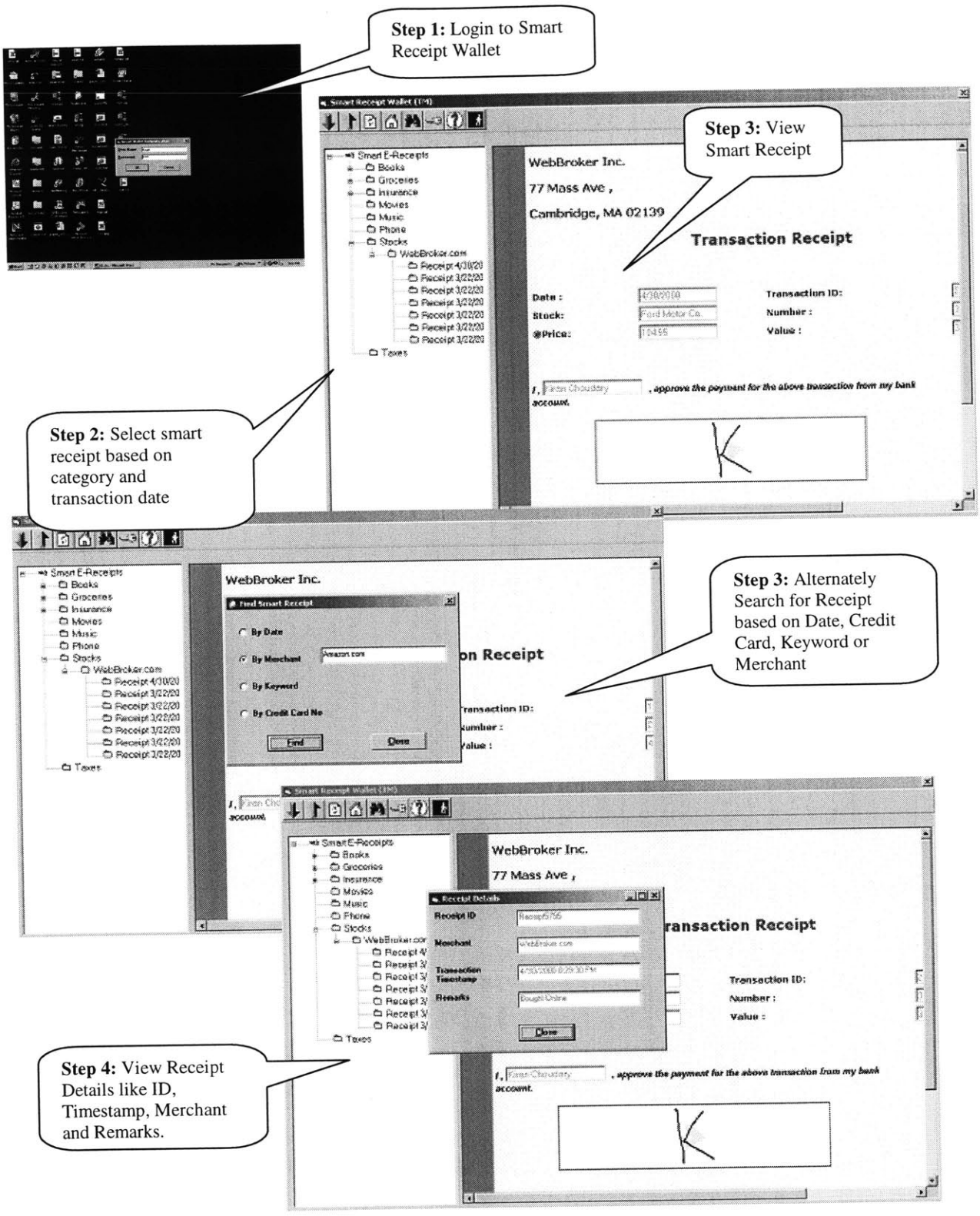


Figure 10-7: Smart Receipt Wallet

10.6 Customized Security Policy

In order to be a feasible alternative to self-implementation of security policies by transaction service providers, the e-Notary service should allow companies to configure their security policy at the e-Notary's service dynamically. Security policies change with e-commerce laws and other business rules and hence the e-Notary should allow transaction service providers to update their policies. The prototype version of the e-Notary allows transaction service providers to develop their security policy and the related user interfaces as part of their registration process (see Figures 10-8, 10-9, 10-10, 10-11).

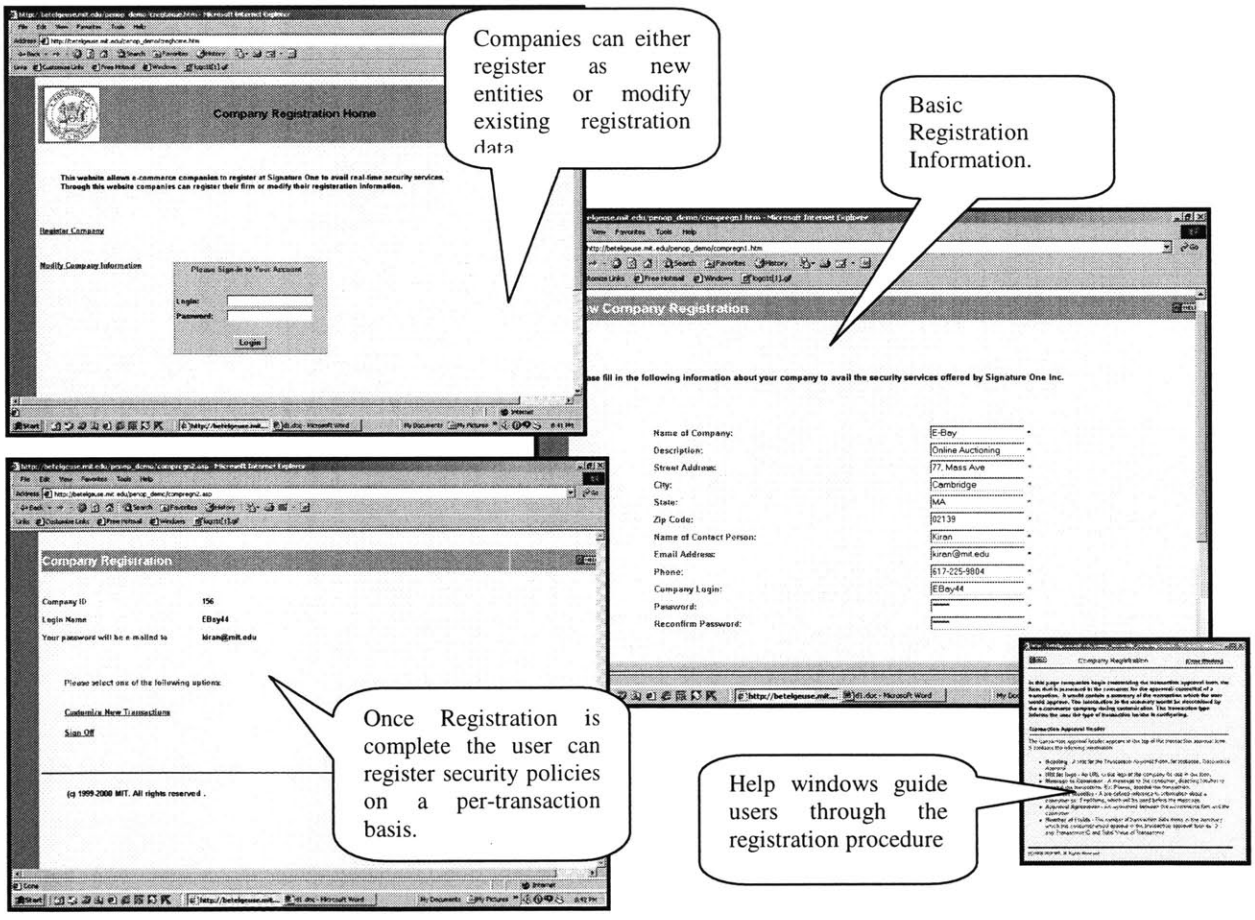


Figure 10-8: Registration Process for Transaction Service Provider

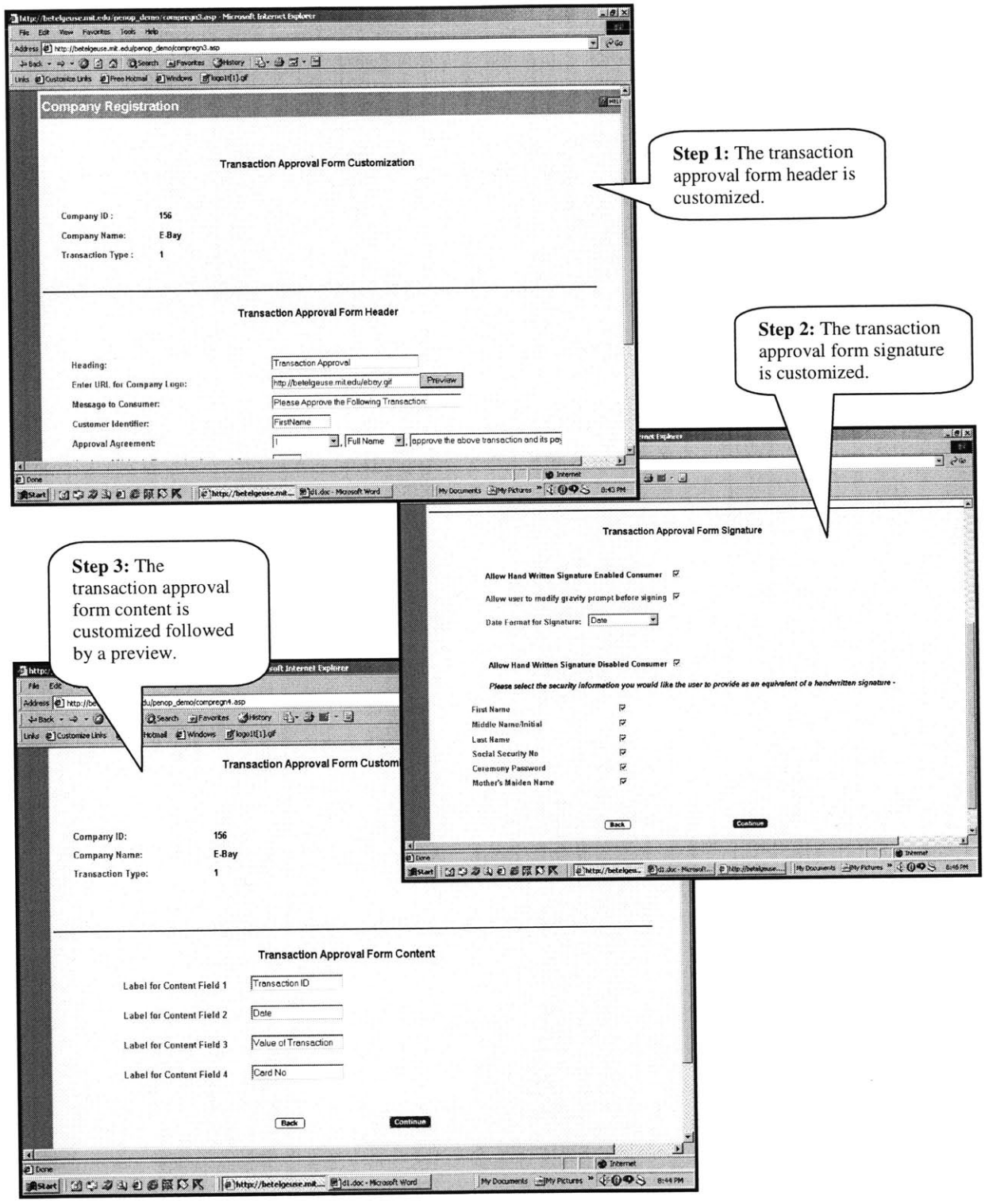


Figure 10-9: Security Policy – Customizing Transaction Approval Form

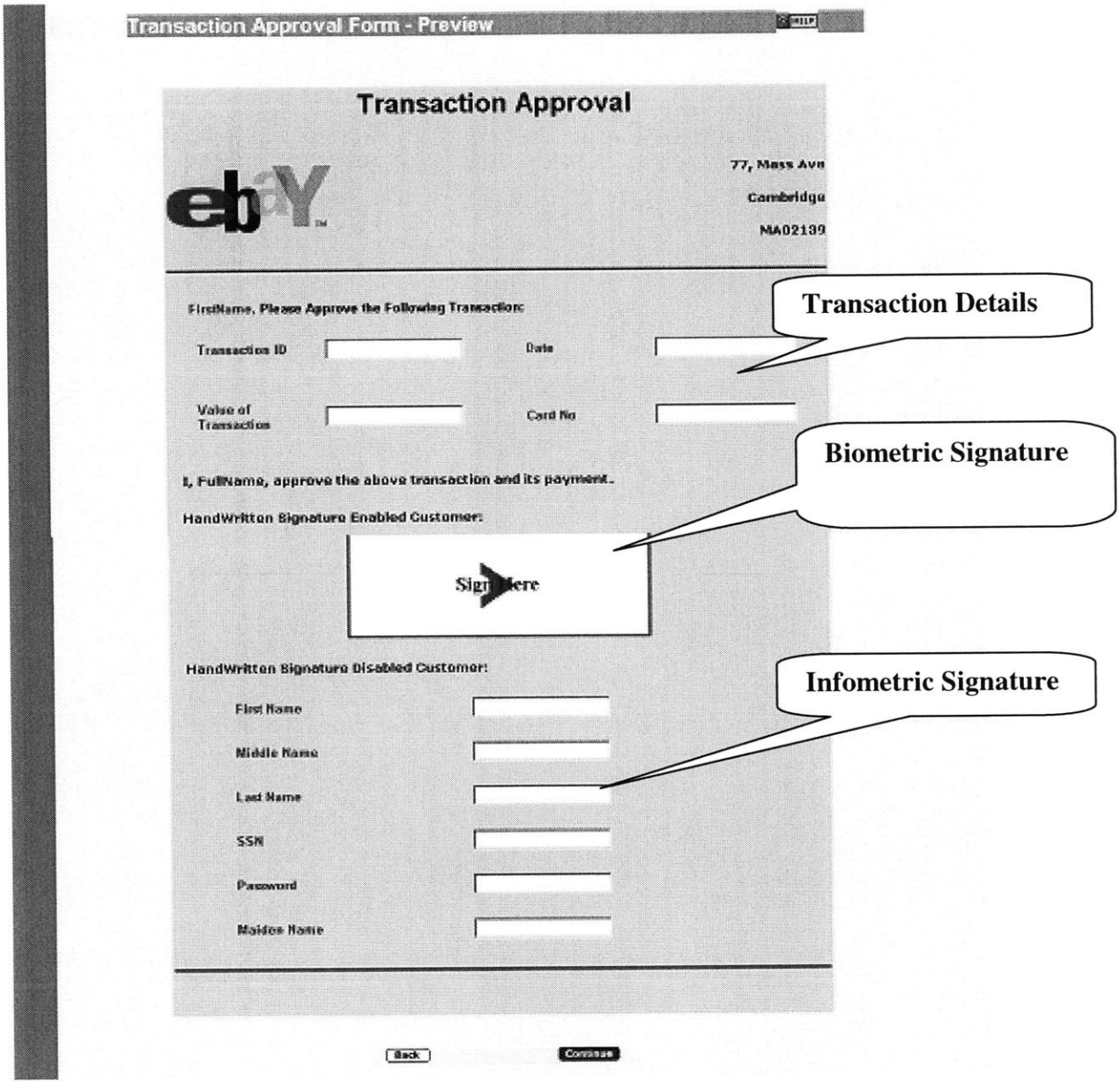


Figure 10-10: Preview of Transaction Approval Form

After the transaction approval form has been customized as part of the security policy, the next step is the customization of the smart transaction receipt (see Figure 10-11).

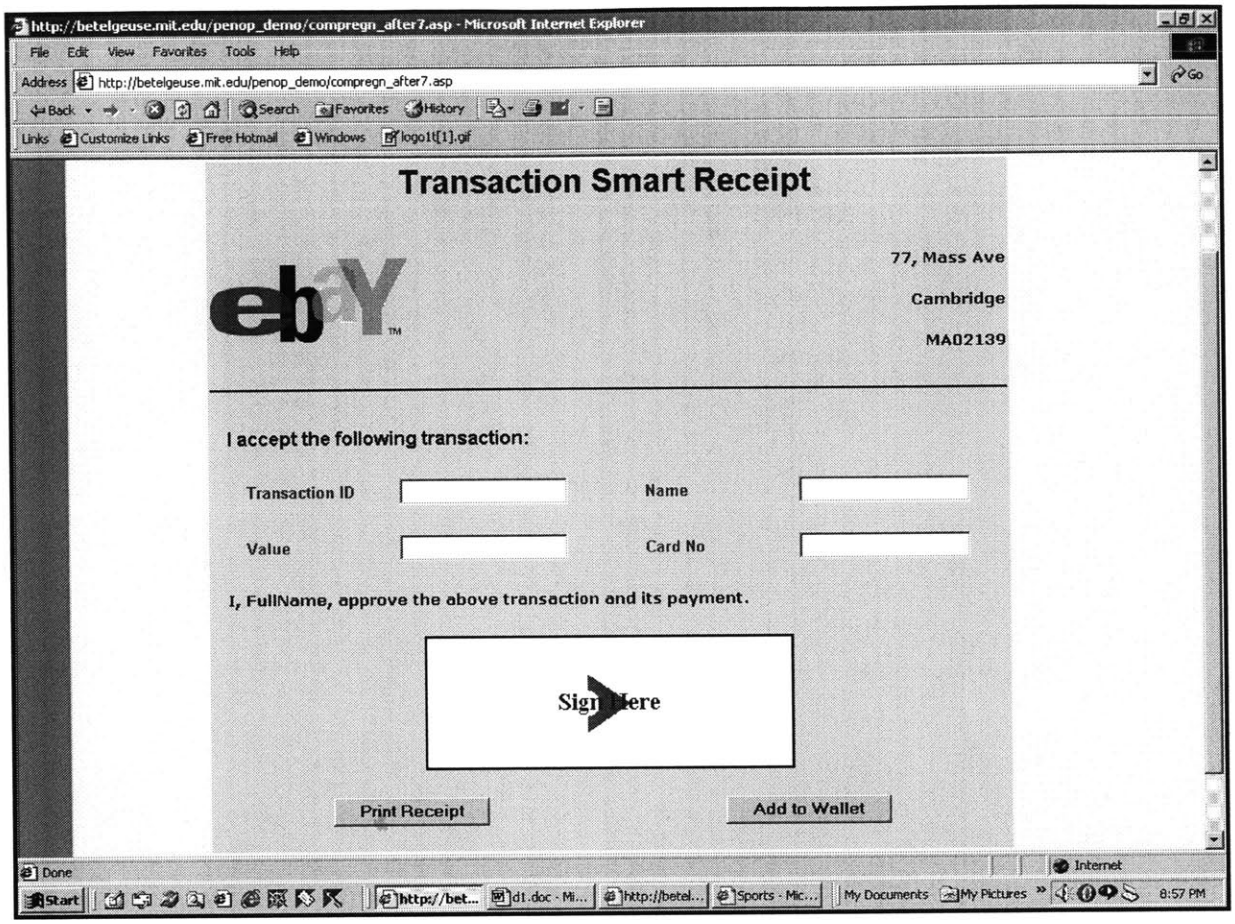


Figure 10-11: Preview of Smart Receipt

10.7 Summary

This chapter discussed the system architecture and components of the prototype version of the e-Notary Service. It then discussed the Smart Receipt and Smart Receipt Wallet that provide users with e-evidence about their electronic transactions. Later, a web-based stockbroker scenario was used as a test case for implementing the prototype version of the e-Notary Service. The next chapter concludes this thesis by providing a review of the research effort; studying the results/ benefits and future scope of this research effort.

Chapter 11

Conclusion

This thesis provides a framework for conducting secure and legally binding electronic transactions. In the first part of the thesis (Chapters 2-7) the focus was on conducting secure and legally binding business-to-business electronic transactions in a specific industry segment namely the $3.2 Trillion [Bidcom, 2000] A/E/C industry. After discussing the security concerns in conducting electronic transactions in A/E/C projects in Chapter 3, a review of the security, that is currently available in web-based project management systems, is conducted in Chapter 4. The approach to developing the framework itself is two-phased. In Chapter 5 a model for secure and reliable communication is developed. This model enables the secure flow of information between the participants of the transaction. In Chapter 6, a model for secure information management is discussed. This model ensures the integrity of the transaction information

beyond the life of the transmission of transaction information. Having developed the framework for secure and legally binding electronic transactions in large-scale A/E/C projects it was applied on a test case, the paper-less office at the $13.6 Billion Central Project at Boston, USA. Chapter 7 discussed the issues related to the implementation of the framework at the Central Artery Project.

Having developed a framework for conducting secure and binding B2B transactions in the A/E/C industry, the thesis then focuses, in the second part (Chapters 8-10) on developing a generic framework for conducting secure and legally binding electronic transactions. The first phase of this research effort, that involved the development of the security framework for the A/E/C industry, served to highlight the security concerns for electronic transactions in general, and also provided some of the technology components needed in a generic framework for conducting secure and legally binding electronic transactions. This contributed to a large extent to the development of a generic framework for conducting secure and binding electronic transactions through the vision of an e-Notary service that provides security services to transactions service providers. Chapter 9 described the vision for an e-Notary service and its functional architecture while Chapter 10 described the system architecture and components of the prototype version of an e-notary service.

11.1 Benefits

Each of the two phases in the research effort, this thesis is based upon, have produced a number of benefits. Most large-scale engineering projects and construction corporations are currently attempting to automate their business processes leveraging the power of information technology (IT). Automating business-to-business (B2B) transactions, between the organizations participating in a large-scale A/E/C project, would not only be a primary requirement, but also a major challenge in their endeavor. The absence of a framework to achieve this has prevented large-scale automation of paper-based transactions across multiple organizations, in spite of the presence of a host of web based

project management services today. The first part of this thesis (Chapters 2-7) addresses this need by developing a framework to implement a system for conducting secure and binding electronic transactions over the Internet. It outlines the security needs of a typical large-scale A/E/C project and the technologies required to address them in order to achieve the transition from paper-based transactions to electronic transactions. It highlights the technology related issues, as well as, organizational issues involved in implementing such a system at large-scale engineering projects like the Central Artery/ Tunnel Project in Boston. In summary, this phase of the thesis would provide IT managers at large-scale A/E/C projects and construction/engineering corporations, as well as, firms involved in providing project management services to the A/E/C industry, with a web-centric architecture for implementing a system to conduct secure and legally binding electronic transactions between organizations participating in A/E/C projects.

The second part of the thesis addresses the security concerns of electronic transactions in general, by developing a web-based e-Notary Service. The e-Notary service would provide security services to web-based transaction service providers enabling them to provide secure and legally binding electronic transactions. This service would not only provide value to the transaction service providers, but also to customers who would now be confident to take part in critical transactions online. It would also serve the security service provider community, who, through strategic partnerships with the e-Notary service, could provide services to the latter's customers.

11.2 Scope for the Future

There is ample scope to build on the work presented in this thesis. This section provides an outline of the future directions this research work can take. The three areas where there is considerable scope for future research are the development of an e-Signature API, XML standards for e-Notary Services and document independent e-Notary services.

11.2.1 e-Signature API

As discussed in Section 9.2.1, e-Signatures can be classified into biometrics, infometrics and PKI-based signatures. There is a need to develop an e-signature API [see Figure 11-1] that would allow the integration of any e-signature mechanism into the e-Notary service with ease, in the future.

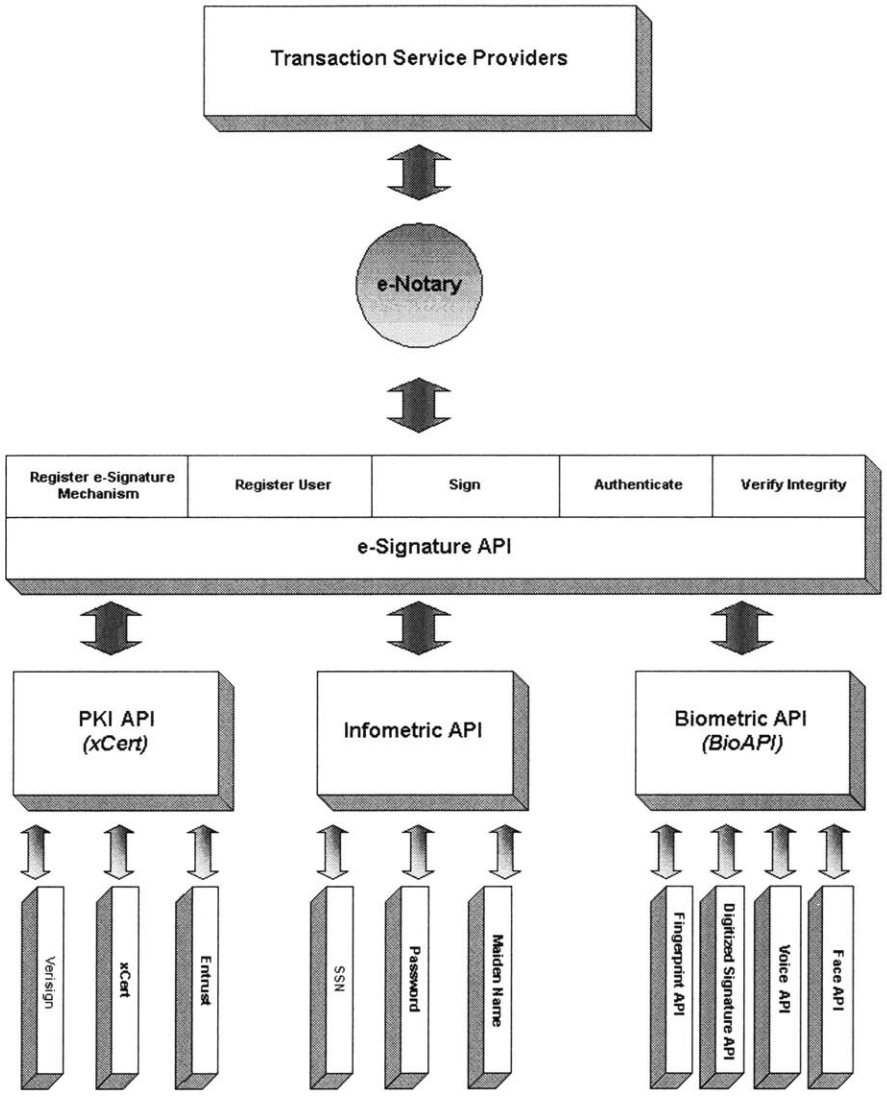


Figure 11-1: e-Signature API

There was been considerable work in the area of development biometric independent APIs and Certificate Authority (CA) independent PKI APIs. The BioAPI Consortium

[BioAPI Consortium, 2000] is working on a specification for developing an OS independent, Biometric independent API. The complete specification is expected in mid 2000. The BioAPI™ would integrate past development in this area namely, the Biometric API (BAPI ™) [I/O Software Inc, 2000] and the Human Authentication API (HA-API) [Biometrics Consortium, 2000]. Xcert Corporation [Xcert International Inc, 2000] has developed an API, the Xcert Development Kit (XDK) that provides a vendor-independent interface to PKI services. Thus there is ample scope to build upon these APIs to create an e-Signature API for the e-Notary service that would allow integration of any e-signature mechanism into the framework for secure and legally binding electronic transactions. The e-signature API would in essence provide the following interfaces -

- *Register e-signature mechanism* – which would allow e-signature mechanisms to register with the e-Notary.
- *Register User-* would allow users to register their e-signatures with a particular e-signature mechanism.
- *Sign* – would capture the e-signature.
- *Authenticate* – would authenticate the user based on the signature capture.
- *Verify Integrity* –would verify the integrity of the signature, as well as, the information approved by the signature.

11.2.2 XML Standards for e-Notary Services

As XML (extensible Markup Language) [XML.org, 2000] emerges as the standard for data interchange in e-commerce applications, it is vital to develop an XML standard for e-Notary Services. In essence a Document Type Definition (DTD) / schema needs to be developed to represent e-evidence in web-based transactions.

11.3.3 e-Document Independent e-Notary Services

Electronic documents vary in function, as well as, vendor (and hence in format). They could range in function from spreadsheets to letters to CAD documents and in vendor

from Microsoft to Adobe to Jetforms. In order to truly replace paper-based transactions the e-Notary service would need to be compatible with most popular documents formats.

Bibliography

1. Adobe Systems Inc. (2000), *develops software solutions for web and print publishing.* (http://www.adobe.com)

2. D. Atkins, P. Buis, C. Hare et-al (1997), *Internet Security Professional Reference*, New Riders Publishing, USA

3. Bentley Systems Inc. (2000), *is a software company that specializes in engineering software and services.* (http://www.bentley.com, March 2000)

4.Bidcom Inc. (2000), *serves the construction industry by providing web based project management services.* (http://www.bidcom.com, March 2000)

5.BioAPI Consortium (2000), *was created to develop an OS independent, Biometric device independent API for application developers.* (http://www.bioapi.org, May 2000)

6. Biometrics Consortium (2000), *serves as the US Government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology.* (http://www.biometrics.org)

7. Buzzsaw.com Inc. (2000), *a subsidiary of AutoDesk Corporation provides web based project management services to the A/E/C industry.* (http://www.buzzsaw.com, March 2000)

8. Center for Democracy and Technology (1998), *Encryption White Paper* (http://www.cdt.org/netcaucus/issues/issueencryptionwhite.html, May 1999)

9. Central Artery/ Third Harbor Tunnel (CA/T) Project, Boston (2000). (http://www.bigdig.com, March 2000)

10. Cephren Inc (2000), *provides collaboration and e-commerce services to the A/E/C industry.* (http://www.cephren.com, March 2000)

11. CISCO Systems Inc (2000), *is a leading manufacturer of networking software and hardware products.*(http://www.cisco.com)

12. Construction Business Systems Australia (2000), *creates software products for project management. (http://www.cbs-aus.com.a, March 2000)*

13. W. Diffie and M. Hellman (1976). "New Directions in Cryptography" *IEEE Transactions on Information Theory*, IT-22: 644-654.

14. Entrust Technologies Inc. (2000) *is a provider of digital certificates and public-key infrastructure (PKI), Digital certificates.* (http://www.entrust.com, March 2000)

15. A. Freier, P. Karlton, P. Koshers (1996) " SSL Specification version 3.0", *Transport Layer Security Working Group, IETF*

16. Framework Technologies Inc. (2000), *develops software products for distributed enterprises and projects.* (http://www.frametech.com, March 2000)

17. Gartner Group (1998), *Business Technology Journal, Inc.* reported on January 20.

18. G. Kyle (1998), *Inside ODBC,* Book News Inc., Portland, OR, USA

19. K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn (1998), "Point-to-Point Tunneling Protocol (PPTP)", *Network Working Group, Internet Engineering Task Force (IETF).*

20. I/O Software Inc, *develops information security solutions and software applications for smart cards, tokens, biometric devices. It developed a Biometric API (BAPI) for application developers.* (http://www.iosoftware.com, May 2000)

21. Internet Engineering Task Force [IETF] (2000), *is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.* (http://www.ietf.org, May 2000)

22. JetForm Corporation (2000), *is developer of secure Web workflow and electronic forms automation providing solutions that streamline business processes.* (http://www.jetform.com, March 2000)

23. B. Kaliski Jr. and M. Robshaw (1995), "Message Authentication with MD5" *CryptoBytes,* (1): 5-8, 1995.

24.K. Lassesen (1995), Microsoft Developer Network Technology Group, "Introduction to Using the Remote Data Object", *MSDN.* (http://premium.microsoft.com/msdn/library/techart/msdn_intrordo.htm, May 1999)

25. M.Laroche (2000), "A Common Criteria Evaluation for a Trusted Entrust/PKI", *Entrust Technologies White Paper* (http://www.entrust.com/products/criteria_eval.pdf, March 2000)

26. T. Li (2000), " Workflow in Large Scale Engineering Projects", *Master of Science Thesis,* MIT

27. Microsoft Corporation (2000), *a software company, specializing in software products for personal computers.* (http://www.microsoft.com, March 2000)

28. MIT Project Athena, "Kerberos: The Network Authentication Protocol", Jan 2000 (http://web.mit.edu/kerberos/www/)

29. Modern Continental Companies Inc (2000), *is one contractors with the largest number of contracts on the Central Artery Tunnel Project at Boston.* (http://www.moderncontinental.com, March 2000)

30. Netscape Corporation (2000), *original developers of the Secure Socket Layer (SSL), now an Internet security standard.* (http://www.netscape.com , March,2000)

31. MSDN (1999), *"Programming with ODBC".* (http://premium.microsoft.com/msdn/library/sdkdoc/boguide/sql_4cir.htm, May 1999)

32. Oracle Corporation (2000), an information management software company specialized in database related software products.(http://www.oracle.com , March 2000)

33. Oracle Press (1998), *Oracle Server Documentation,* Oracle Corporation, Redwood City, CA

34. F. Peña-Mora, R. Sriram, and R. Logcher, (1995) "Conflict Mitigation System for Collaborative Engineering", *AI EDAM - Special Issue of Concurrent Engineering,* Vol.9, No.2.

35. F. Peña-Mora, S. Vadhavkar, E. Perkins and T.Weber, (1999) *"Strategic Information Technology Planning Framework for large-scale A/E/C Projects", ASCE – Journal of Computing in Civil Engineering,* October 1999

36. PenOp Inc (2000), *is a developer of electronic signature technology that enables secure e-commerce. Their products include the Penop Signature Series, Penop Signature Plugins and the Penop Signature Toolkit API.* (http://www.penop.com, March 2000)

37. Penop Inc (1998), *Penop SDK Documentation.* (http://www.penop.com, March 2000)

38. Penop Inc (1998), *Penop Signature Plug-in for MS ™ Word documentation.* (http://www.penop.com, March 2000)

39. Penop Inc (1999), *Penop Signature Plug-in for Adobe Acrobat documentation.* (http://www.penop.com, March 2000)

40. Perkins Coie LLP (2000*) is a law firm that specializes in Internet and E-commerce law. They maintain an index of e-commerce legislation on their corporate web site.* (http://www.perkinscoie.com/resource/ecomm/digsig/index.htm, March 2000)

41. Primavera Systems Inc.(2000), creates software products for project management. (http://www.primavera.com, March 2000)

42. PrivacyExchange.org (2000), is a free global information resource web-site on consumer privacy, e-commerce and data protection. (http://www.privacyexchange.org, March 2000)

43. RSA Data Security, Inc. (2000), *is a developer of cryptography products. RSA technologies is part of existing and proposed standards for the Internet and World Wide Web, ITU-T, ISO, ANSI, IEEE, as well as business, financial and electronic commerce networks worldwide.* (http://www.rsa.com, May 2000)

44. Resource International Inc (RII), (2000), *is a civil-engineering firm that specializes in IT solutions for project management.* (http://www.projectgrid.com, March 2000)

45. E. Smith, V. Whisler and H. Marquis (1998), *Visual Basic 6 Bible*, IDG Books, Foster City, CA, USA

46. Sun Microsystems Inc. (2000), *is the creator of the Java Programming Language.* (http://www.sun.com)

47. K. Unkroth (1998), *Microsoft Exchange Server Training,* Microsoft Press, Seattle, WA, USA

48. VeriSign, Inc. (2000), *is one of the providers of Public Key Infrastructure and digital certificate solutions used by enterprises, Web sites, and consumers to conduct secure communications and transactions over the Internet and private networks.* (http://www.verisign.com, March 2000)

49. Xcert International Inc., *is a provider of Internet-based Public Key Infrastructure (PKI) solutions and the developer of Xcert Development Kit (XDK) which is an API for integrating PKI services.* (http://www.xcert.com, May 2000)

50. XML.ORG (2000), *is an independent resource for news, education, and information about the application of XML in industrial and commercial settings.* (http://www.xml.org, May 2000)