Access With Trust

This document is available electronically at gits.gov

September 1998

Federal Public Key Infrastructure Steering Committee

Government Information Technology Services Board

Office of Management and Budget

Access With Trust

This document is available electronically at gits.gov

September 1998

Federal Public Key Infrastructure Steering Committee

Government Information Technology Services Board

Office of Management and Budget

Table of Contents

Letter to the Citizens

Executive Summary

Section 1. Introduction 1
1.1 Background 1
1.2 Purpose of Report 2
1.3 Structure of Report 3

Section 2. The PKI 5
2.1 Need for a PKI 5
2.2 Description of the PKI 5
2.3 Vision 7

Section 3. Environmental Factors and Forecast 9
3.1 Business 9
3.2 Government 9
3.3 Regulatory 11
3.4 Public Acceptance and Agency Readiness 13
3.5 Explanation of Public Key Technology 14

Section 4. Principles Governing Federal Role in PKI Development 17
4.1 Exercise Federal Leadership 17
4.2 Use Commercially Available Technology and Products 17
4.3 Support Multiple Technologies and Promote Interoperability 19
4.4 Work Closely with Industry and Other Parties 19

Section 5. Strategy and Actions 21
5.1 Security/Privacy Requirments 23
5.2 Standards and Planning 23
5.2.1 Support Pilot and Demonstration Projects 23
5.2.2 Support Resolution of Policy Issues 24
5.2.3 Articulate Specifications and Standards 24
5.3 Education 24
5.3.1 Educate Government Personnel on the New PKI 24
5.3.2 Become a Promoter and Focal Point 25
5.4 Demonstration of the PKI 26
5.4.1 Demonstrate Potential Uses of the Emerging PKI 26
5.4.2 Promote the Development of Common Foundations 27
5.4.3 Continue Partnership with Industry 28

TABLE OF CONTENTS (CONTINUED)

5.4.4 Explore Encryption Key Recovery 28
5.5 Other Issues 29
5.5.1 Identity Proofing 29
5.5.2 Interoperability 30
5.5.3 Liability 30
5.5.4 Fraud Protection and Prosecution 31
5.5.5 Records Management and Archival Preservation 31

Section 6. Accomplishments 33
6.1 Federal PKI Outreach 33
6.2 Steering Committee's Working Groups 34
6.2.1 Technical Working Group 34
6.2.2 Business Working Group 35
6.2.3 Legal and Policy Working Group 36

Section 7. Membership of the Federal PKI Steering Committee 37

Section 8. List of Acronyms 39

Appendices
Appendix A. Essential PKI Management Functions 43
Appendix B. Overview of the PKI Pilot Projects 45

List of Figures
Figure 3.2 Doing Business with the Federal Government 10
Figure 5.1 PKI Strategy 23

Dear Citizen:

The growth of communications networks and increasing use of the Internet provide the Federal government with unique opportunities for improving service to Americans.

Last year, Vice President Al Gore and the National Partnership for Reinventing Government issued *Access America*, a report outlining steps to encourage and increase Internet access to government services by 2000. The report says:

> *Public confidence in the security of the government's electronic information and information technology is essential to creating government services that are more accessible, efficient, and easy to use. Electronic commerce, electronic mail, and electronic benefits transfer sensitive information within government, between the government and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, assure that the information is not altered in an unauthorized way, and be available when needed.*

This report, *Access with Trust*, describes an essential technological and institutional means of fostering safe, secure electronic interactions, a Public Key Infrastructure or "PKI." *Access with Trust* focuses on how the Federal government will promote and use a PKI to safeguard and protect electronic interactions internally (among Federal government employees and agencies) and externally (between the Federal government and its many trading partners-state and local governments, businesses, and individuals).

Our partners in this effort will be other governments (domestic and foreign), colleges and universities, banks and other businesses, and non-profit organizations and advocacy groups, as well as those private-sector technology providers from whose products and services the infrastructure is built. In other words, this will be a collaborative effort, not a "government" solution or even one in which the government plays the principal role.

We hope that *Access with Trust* will help you learn more about how this important technology is providing Americans with secure and private electronic access to government services.

Greg Woods
Chair, Government Information Technology Services Board

G. Edward DeSeve
Acting Deputy Director for Management
Office of Management and Budget

Richard Guida
Chair, Federal PKI Steering Committee

EXECUTIVE SUMMARY

In a democracy, government exists to serve and protect its citizens and their institutions. How government delivers on its obligations must continually evolve. A recent evolutionary change is the need for government to support and promote an electronic means of communicating and interacting with citizens and companies, to make government work better and cost less. With over sixty million adults in the United States alone having access to the Internet, and thousands of U.S. companies hosting sites on the World Wide Web, interacting with the government electronically ("electronic government") can affect a wide diversity of constituents in profound ways.

Access America[1] is Vice President Gore's 1997 report outlining steps to encourage and increase citizen and business access via the Internet to the most commonly requested government services by 2000. To make this vision a success, the American people must have confidence that government systems with which they interact electronically provide adequate security and privacy safeguards.

This report, *Access with Trust*, describes Federal government goals and efforts to develop a Public Key Infrastructure (PKI). Properly implemented in concert with other security services, the PKI serves as a fundamental building block for a broad spectrum of electronic commerce and government communications, all done in a fashion which protects the privacy of citizens and companies and gives them the confidence to use this new medium of communication routinely, frequently, and effectively. The report discusses the value of a PKI, and how the Federal government is promoting one through a careful process of adopting and implementing standards in cooperation with industry, articulating sound business practices governing agency use of the PKI, and conducting pilot demonstration projects to explore the many ways in which public key technology can enhance agency operations and interactions with citizens and companies. The report further describes how the Federal government's efforts are ultimately intended to complement the many projects which private industry is pursuing using public key

1. *Access America, Reengineering Through Information Technology*, Report of the National Performance Review and the Government Information Technology Services Board, Vice President Al Gore, February 3, 1997, available at gits.gov.

technology for business applications, and to provide a more secure environment for the operation of government information systems.

While many of the concepts underlying the technology are complex, the principles derive from common sense and are explained within the report so that those interested in the matter can read and understand them, and thus become informed consumers of the capabilities which PKI affords.

The authors of this report, representing virtually every major Federal agency, hope that it fulfills the needs of each person who reads it, just as the PKI which the report describes will meet the needs of all who use it.

SECTION 1. INTRODUCTION

1.1 Background

Electronic transactions can only flourish in a trusted environment.

The growth of communications networks, the increasing use of the Internet for commercial and private purposes, and the application of computers to an ever expanding number of tasks, all provide the Federal government with unique opportunities for improving service to the American people. Through the National Partnership for Reinventing Government (NPR) and associated agency reinvention efforts, a new vision of government is emerging, one where residents will use electronic pathways to get government information and services, will communicate their views electronically, and will get quick and accurate answers to their questions.

Examples of Electronic Services and Information:

- Students applying for loans on-line, and using their school-issued identification cards to do business with the government over the Internet.
- Parents checking the performance of schools and the environmental quality of neighborhoods when looking for a new home.
- Adults getting information on medications or paying their taxes without leaving home.

Over sixty million U.S. citizens have access to the Internet, and thousands of U.S. companies host sites on the World Wide Web, so the potential utility of this medium for government and business purposes is obvious. And there is substantial room for growth. In the commercial sector, only 13 percent of U.S. users made purchases over the Internet in 1997, and total purchases were estimated at $4 billion - less than one percent of all consumer retail sales. Thus, while many consumers use the Internet to become better informed, concerns over privacy and security have affected its use as a medium for purchases.

Access America[2] is Vice President Gore's 1997 report outlining steps to encourage and increase citizen and business access via the Internet to the most commonly requested government services by 2000. To make this vision a success, the American people must have confidence that government systems with which they interact electronically will provide adequate security and privacy safeguards. As the report says:

> *Public confidence in the security of the government's electronic information and information technology is essential to creating government services that are more accessible, efficient, and easy to use. Electronic commerce, electronic mail, and electronic benefits transfer sensitive information within government, between the government and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, assure that the information is not altered in an unauthorized way, and be available when needed. A corresponding policy and management structure must support those protections.*

To achieve the vision, participants must be able to trust this new way of doing business. Both service providers and customers must be able to get and provide information and conduct other transactions with the confidence that security and privacy will be maintained. To facilitate this access with trust, all partners — the Federal government, states, localities, businesses, banks, schools, and citizens — must find ways to cooperate in building a public key infrastructure to promote and support these new relationships.

1.2 Purpose of Report

This report is entitled *Access with Trust* because it describes an essential component of the emerging technological and institutional environment in which trust can flourish. This component is called a *Public Key Infrastructure* or "PKI" because it is based on a security technique called "public key cryptography." The infrastructure fosters safe, secure interactions between parties involved in an electronic transaction.

Access With Trust describes how the use of public key technology can help create a trusted electronic environment.

2. *Access America, Reengineering Through Information Technology*, Report of the National Performance Review and the Government Information Technology Services Board, Vice President Al Gore, February 3, 1997, available at gits.gov.

Access with Trust focuses on how the Federal government will promote and use a PKI to safeguard and protect electronic interactions internally (among Federal government employees and agencies) and externally (between the Federal government and its many trading partners — governments, businesses, and individuals). But the principles set forth here, and the steps and tasks identified, do not involve the Federal government alone. Our partners will be other governments (domestic and foreign), colleges and universities, banks and other businesses, and non-profit organizations and advocacy groups. In particular, our partners will include those private-sector technology providers from whose products and services the infrastructure is built.

The central organization representing the Federal government in this effort is the *Federal Public Key Infrastructure Steering Committee* ("Steering Committee"), which operates under the Government Information Technology Services Board, a body established under Presidential Executive Order 13011 to promote the use of information technology within Federal agencies to improve services and reduce costs. Building upon efforts completed to date, the Steering Committee is working with other groups within and outside the government to promote and implement ambitious PKI applications to show how this technology can support government functions and activities in a world of trustworthy electronic communications.

1.3 Structure of Report

Access With Trust is intended for a variety of audiences. Members of Congress and their staffs may find this report helpful in better understanding the emerging PKI and some of its legislative and policy ramifications. Senior administration officials may find it useful when drafting policies dealing with the PKI. Companies which provide or use telecommunications or data processing services may glean information helpful to their interests. Finally, anyone interested in learning more about the PKI should find this report useful.

This report covers four specific areas:

- Basic security services and functions to be provided as part of the PKI;
- The Steering Committee's role in supporting and helping to develop the Federal portions of the PKI;
- How external factors are shaping the future of the PKI; and
- The status of the PKI today, along with current Federal government plans for building and using this infrastructure.

SECTION 2. THE PKI

2.1 Need for a PKI

The challenges in processing, transmitting, and storing information in a fashion which protects its authenticity, integrity and confidentiality have been well publicized and have become part of the public debate on the future of communications in general and "The Information Superhighway" in particular. The Federal government must meet those challenges while supporting the NPR's goal of modernizing Federal government business processes by conducting those processes electronically. Accomplishing these objectives requires the proper and timely use of security services so that businesses and the public operate in a trusted environment. Development and implementation of the PKI helps provide that trusted environment.

A Public Key Infrastructure (PKI) provides the elements needed for a trusted environment.

Research and pilot projects performed in recent years have shown that the PKI will need to use public key technology and standards, be fully interoperable among agencies and applications, and be recognized internationally. In the near term, the government will use the PKI in support of the NPR goals. The PKI will be used primarily to authenticate users and data, protect the integrity of transmitted data, and ensure the non-repudiation and confidentiality of data. Other necessary security measures, such as protection against unauthorized access to systems and data, will be provided through separate security mechanisms and policies. Used in conjunction with these security mechanisms and policies, the PKI will form an important part of the basis for the trusted environment needed for transactions with the public and other trading partners to proceed.

2.2 Description of the PKI

The PKI is not only software or hardware. It is an *infrastructure*, that is, a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions on open networks such as the Internet. It is not a single monolithic entity, but a distributed system in which the component elements may include multiple agency-specific public

key infrastructures which are interoperable and interconnected. The infrastructure provides assurances that information is protected while being entered, during transit, and when stored. The underlying technology is already developed by private industry and is being marketed and used commercially. The PKI promotes interoperability among commercial products and the early integration of security features into those products.

A critical goal in developing the PKI is ensuring that it meets the needs of its users without undue complexity or cost. This is no small matter, because potential users represent a broad spectrum, ranging from those who need a modest level of security and cannot tolerate substantial expense for that purpose, to those who need much higher levels of security and are willing to incur the expenses associated with those services. The PKI will need to be extensible, that is, capable of satisfying this spectrum of users and accommodating the environments in which they operate.

For more detailed information about public key security services and functions, please refer to Appendix A.

Through digital signatures and encryption, the PKI will provide four basic security services:

- *Authentication* — Ensure that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information.
- *Data Integrity* — Ensure that data is unchanged from its source and has not been accidentally or maliciously altered.
- *Nonrepudiation* — Ensure strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and, to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data.
- *Confidentiality* — Ensure that information can be read only by authorized entities.

2.3 Vision

The PKI described in this report will be a foundation supporting trusted communication among Federal government agencies and between those agencies and state or local government, the public, and private companies. As described above, however, the PKI cannot be a "government-only" approach; it will depend on and interface with the larger, evolving private sector PKI that supports interactions among individuals, companies, and organizations where there is no direct Federal government presence. Thus, the PKI discussed in this report must be designed and built in close cooperation with the private sector.

The PKI must be designed and built in close cooperation with the private sector.

Bearing in mind the needs of Federal customers, the PKI must be secure, reliable, flexible, cost-effective, and provide a level of assurance based on the requirements of each application while ensuring proper privacy protection. To accomplish these goals, the Federal government must:

- Identify its own business requirements and the requirements of its customers;
- Prepare and implement appropriate standards in cooperation with industry;
- Articulate sound business practices governing agency use of the PKI;
- Conduct pilot demonstration projects to explore the many ways in which public key technology can enhance agency operations and promote interactions with citizens and companies;
- Define and develop, in cooperation with the private sector, the model policies, contracts, and other security services necessary to ensure the maturation and more expansive use of the PKI; and
- Develop and implement mechanisms to measure the Federal government's progress in accomplishing PKI goals.

SECTION 3. ENVIRONMENTAL FACTORS AND FORECAST

To understand government efforts to develop a PKI requires understanding first the underlying environment which the PKI is intended to serve, and a few simple technical concepts common to public key technology.

3.1 Business

In the private sector, the ability to interact and exchange information electronically within a company, along with conducting electronic commerce over the Internet, has drastically changed how business is done. Entire management layers are now being replaced with distributed management models that allow information to be disseminated quickly throughout an organization. Instead of reporting to the office each day, many employees now work from home or from a customer's site, exchanging messages and other information via the Internet. Individuals and companies worldwide can now transact business with each other over the Internet. Important industry markets, such as banking — a pioneer in using technology to improve service to its customers — are now investing heavily in advanced technologies to offer such services as Automated Teller Machines (ATMs), Electronic Funds Transfer (EFT), and Debit/Credit Cards.

Convenience, efficiency of operation, and customer satisfaction drive businesses to use electronic commerce.

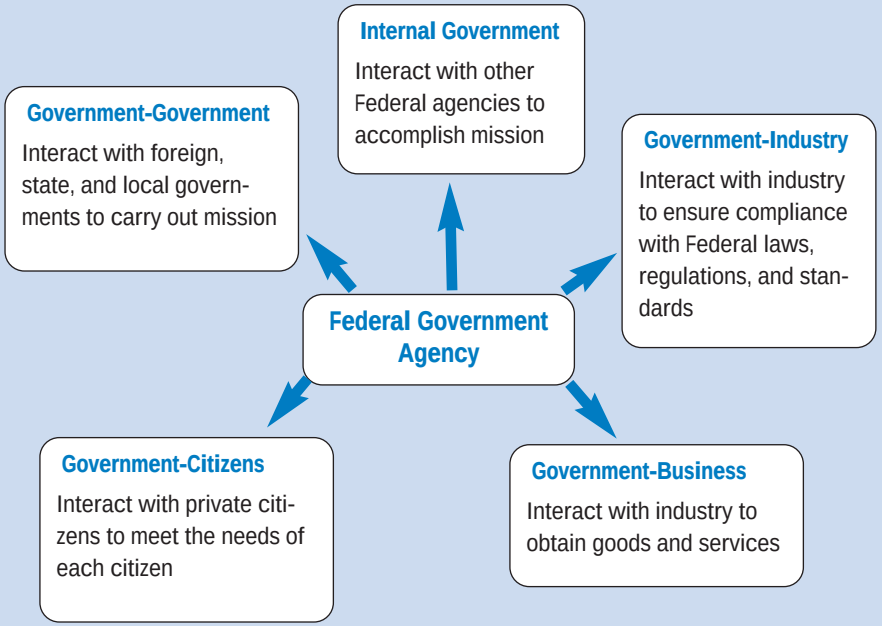
Individuals now expect to be able to interact electronically with businesses, expect to use banking services from their homes, and expect industry to update frequently those products which serve these functions to provide greater capabilities. Businesses risk losing customers and market share if they fail to provide such services.

3.2 Government

The same customers who use business services expect commensurate service from all levels of government. If they can interact electronically with businesses using open networks, they should be able to interact with government in the same manner. Consumers

The same desires and advantages are driving the Federal government to offer electronic services to citizens.

FIGURE 3.2
DOING BUSINESS WITH THE FEDERAL GOVERNMENT



should not have to wait days or weeks to get needed information or benefits. Fortunately, electronic mechanisms allow government to provide those services in a timely and efficient fashion. Thus, much like industry, the government in general, and the Federal government in particular, must transform itself so that it too can benefit from what technology offers.

The Federal government has a large and diverse customer base with which it needs to interact. As shown in Figure 3.2, the government's customers range from individual citizens, who may require infrequent interaction, to large corporations, who may interact often and in a variety of ways. It does not matter with whom the government interacts, how frequent the interaction is, or how the interaction is accomplished; the government is always expected to provide, and should provide, high quality service in a timely manner.

Just like the private sector, the Federal government is under pressure to streamline its business processes to allow it to take advantage of the opportunities the PKI provides. Governments are the

largest creators, collectors, users, and disseminators of information. Sound scientific research, public health and safety, environmental protection, the nation's defense, and the equitable collection and distribution of tax receipts are a few of the national priorities that depend on Federal information systems. The Federal government must identify and implement new business processes to use the PKI to improve delivery of important government services to its citizens in a trusted environment.

3.3 Regulatory

Today's business practices within the Federal government, state and local government, and private industry are backed by several hundred years of legislative, regulatory and judicial actions, decisions, and policies designed to protect parties from loss or fraud in a business transaction. Most of these business practices are so well understood and routine — like written signatures and certified mail — that we rarely think about the legal or other functions they accomplish. Thus, statutory and regulatory provisions commonly specify that communications be "in writing," "signed," "verified," or "acknowledged." These principles have become so universal that most routine paper-based communications, particularly forms, contain a requirement for a signature even in the absence of any specific legal or administrative directive that an original autograph signature actually be affixed. Yet, while meeting legal requirements may hinge on the written signature, the underlying trust relationship between the parties rarely does.

Electronic transactions depend upon a trusted environment, where information is kept confidential, its integrity is ensured, users can be authenticated, and transactions cannot be repudiated.

In electronic communication environments, trust techniques must be designed to satisfy each party to the transaction. In effect, the trust relationship must be supported as part of the transaction for the parties to accept that transaction as valid. At a minimum, the following four requirements must be satisfied to ensure a trusted electronic transaction:

- The information sender and information recipient need to be identified so the parties know where the information is coming from and that it is going to the right party.

- The parties must be confident that the transmitted information was not altered.
- In case of a legal dispute, there has to be a way to establish that the sender sent the information and that the recipient received the information.
- If confidentiality is necessary, the information needs to be protected from unauthorized access during transit.

These requirements correspond to the security services that the PKI will provide (see Section 2.2). A PKI which satisfies these four requirements will support Federal government assurances to its citizens and its trading partners that transactions are trustworthy.

How will the Government use the PKI?

- To improve the public's access to government services and information;
- To improve the flow of information within and among the different levels, branches and agencies of government;
- To reduce government operating costs while improving the quality of the service; and
- To improve the security of unclassified government information systems.

Many initiatives are underway to promote secure electronic service delivery and practices within the United States. Many international, Federal, State, and private sector organizations are addressing domestic and international laws and policies. The American Bar Association and the American Bankers Association are keenly interested in helping define the use and potential impacts of the PKI. While State and Federal legislative and executive bodies consider how to promote secure electronic transactions, other organizations — government, academic, and professional — are developing formal or de-facto standards for electronic service delivery.

With this evolutionary process underway, the Federal government must face a number of legal and policy challenges ranging from the legal structure of the business relationships between the providers

of this technology and the people who rely on it, to the liability and consumer protection standards which will apply. While some have suggested that Federal legislation is timely in this area, it may be wiser to accept the view of others who continue to consider the issues and problems carefully, and then come to a consensus as to their best resolution, before moving forward with legislation.

3.4 Public Acceptance and Agency Readiness

The impact of computerization on commerce will be as great as that of the industrial revolution. Electronic messaging and Internet-based techniques, hold great promise to become the preferred methods of communicating administrative and business information.

The public has shown that it is increasingly willing to use the Internet and other electronic means to transact business. While these transactions often involve private information, some may need lesser degrees of protection than others. For example, ordering free government or commercial publications may require less protection than purchasing materials from the government or transferring funds using a credit card. In many transactions, it is important that the least amount of information about the requester be required and provided so as to preserve privacy. In general, the widespread use of techniques for electronic service delivery will occur only if the transactions actually have, and are perceived to have, a degree of security which is at least as good as equivalent paper-based delivery systems. In many cases, the actual and perceived levels of security will need to be far higher to allay concerns about relying on new technology to conduct transactions.

To succeed, the PKI must provide a level of assurance for users which is greater than that afforded by security measures currently in place.

While the Internet has been an effective distribution channel for general information, using it for financial or confidential business communications will be made easier by the spread of PKI services. The general public is already starting to benefit from such services as they are used by the automotive, financial, and credit card industries.

While the Federal government gradually implements the use of PKI, it will continue to use other identity mechanisms, such as Personal Identification Numbers (PINs) and passwords. These are among the interim security measures for completing financial transactions electronically in the business world today (e.g., on-line banking, automatic teller machines). Most individuals have at least one PIN

and password that they use regularly. To provide an added measure of integrity and confidentiality to these transactions, some service providers and recipients elect to use encryption to supplement the security of PINs and passwords.

PINs and passwords represent useful but rudimentary and incomplete forms of electronic authentication. Although PINs and passwords fail to offer the complete set of benefits of a public key approach (confidentiality, integrity, authentication and nonrepudiation), they nonetheless allow Federal agencies to move away from traditional "pen-to-paper" methods, thereby reducing the cost, delay and complexity associated with that form of authentication. Indeed, where it is possible to verify the identity of a service or benefit recipient (through face-to-face authentication or some other means of establishing identity), PINs and passwords may support better fraud detection and prevention than pen-to-paper signatures. As a result, many Federal agencies, especially those with heterogeneous client bases with varying degrees of technological sophistication, may choose to use PINs and passwords as interim steps. Over time, it will be possible to supplement or replace these forms of electronic authentication with other elements of the PKI to facilitate the transition from paper-based authentication.

3.5 Explanation of Public Key Technology

Public key technology depends upon complicated mathematical concepts but it has a simple, understandable effect: When an individual (we will call him "Bob") starts to participate in the PKI, he begins with a pair of "keys," which look like very long character strings and are actually digital representations of very large numbers. These keys are either chosen by Bob or provided through trustworthy mechanisms, subject to certain mathematical requirements. One of these keys is secret (private) and the other is published (public).

Public key technology uses two "keys" (character strings) that are mathmatically bound. One is kept private, the other is made public, and the former cannot be deduced from the latter.

The essence of public key technology is that messages or transactions authenticated or encrypted using one of Bob's keys can only be verified or decrypted using his other key. Thus, when Bob uses his private key to sign an electronic message or other transaction digitally, anyone who knows Bob's corresponding pub-

lic key can verify Bob's signature. A similar method using public key technology can be used to encrypt messages for confidentiality, and then decrypt them.

The evolving PKI will use special digitally-signed documents (called "certificates") to bind Bob's identity to his public keys. Digital certificates are provided by a trusted "Certification Authority" (CA) and signed using that CA's private key. When someone else (we will call her "Alice") wants to obtain with certainty Bob's public key, she may get Bob's certificate from Bob in person, or she may get it from an on-line "repository" for certificates, or even from Bob's homepage on the World Wide Web. Where or how Alice gets Bob's certificate is not important, because she validates the certificate by validating the CA's digital signature. Alice now knows Bob's public key and name with certainty and can validate any messages sent to her which were signed with Bob's private key. These transactions may be conducted with assurance even though Bob and Alice may have never met.

To validate the CA's signature on Bob's certificate, Alice must first know the public key of Bob's CA. Alice only needs to know the public key of one CA that she trusts. CAs may issue certificates to each other. If Alice does not know the public key of Bob's CA, she can find a certificate issued by a CA whose key she does know, that will certify the public key of Bob's CA. Much of the challenge of building a robust global PKI is in the management of certificates among CAs, as well as the software and infrastructure that automate the process of building and validating these trust chains of certificates. A Model Certificate Policy document for Federal government use is being prepared to promote this process, discussed further in Section 5 below.

As a general matter, good security practices will permit and encourage Bob to have different public-private key pairs for signature and confidentiality uses, and to reflect his different roles (e.g., as an agency official, and as a private citizen and consumer). This is analogous to a person having different passwords for use on different computer systems, or different PINs for use with different financial accounts.

The scientific, academic, and business communities recognize that the capabilities described above provide the best way to replace handwritten signatures in the electronic world, to authenticate identities securely, and to maintain confidentiality on open networks.

To realize this vision of transacting electronic business with security and privacy, it is critical that the various implementations of public key technologies work together smoothly and in a fashion transparent to the user. Neither Bob nor Alice should have to study cryptography to use the technology with comfort and ease!

Section 4. Principles Governing Federal Role in PKI Development

4.1 Federal Leadership

The emerging PKI must satisfy a diverse set of Federal program requirements. To ensure that it does so, the Government Information Technology Services (GITS) Board established a formal government-wide committee, known as the Federal Public Key Infrastructure Steering Committee, to provide leadership within the Federal government during development and implementation of the PKI. The Steering Committee, chaired by the GITS Board Champion for Security, comprises senior-level representatives from all involved Federal agencies.

The Federal Public Key Infrastructure Steering Committee works to coordinate Federal agency activities and make them interoperable.

The Steering Committee believes that the Federal role in developing and promoting the PKI must be guided by the following principles:

- The Federal government must use commercially available technology and products which support the goal of demonstrating, on a convincing scale with a diverse set of applications and customers, that the PKI can transform the manner in which individuals and organizations interact with government in beneficial ways;
- The Federal government must encourage industry to build products which are interoperable and extensible, making sure that Federal programs can take advantage of later marketplace changes and improvements;
- The Federal government must support multiple technologies, resisting the temptation to settle on a single "Federal" solution, and in doing so promote a relationship with business, industry, other governments, advocacy groups and other parties to ensure that their interests are understood and considered.

4.2 Use Commercially Available Technology and Products

Even though Federal government and government-related applications for information security represent a large and diverse cus-

Steering Committee Roles and Responsibilities

- Champion the transformation of government programs and services to secure electronic form;
- Promote the development of an interoperable and extensible PKI that uses commercial standards-based products and services in an open (that is, nonproprietary) environment, and with the capability of being scaleable (that is, able to support a much larger base of users);
- Identify, develop, implement and promote pilot applications that:
  - demonstrate the usefulness of public key technologies,
  - work with public and private sector partners,
  - support a variety of security requirements and transaction volumes,
  - support interoperation among applications, creating greater value for our trading partners;
- Provide support and assistance to Federal agencies and organizations in modifying their programs and applications to take advantage of the PKI, including educating senior officials within the government on the uses and benefits of a PKI; and
- Support programs and projects such that efforts are coordinated with other domestic and international bodies.

tomer base for new security and privacy solutions, few of the needs and requirements of the government (particularly in the realm of unclassified information) differ fundamentally from those of the business world. Most security solutions will be developed by private industry and will be offered to a broader customer base as off-the-shelf products or services. Even when there are unique, government-specific security infrastructure requirements, privately developed and commercially offered solutions may satisfy such needs.

The Federal government wants to use and promote the development of commercial products for its PKI.

The selection of commercially available technology and products should help demonstrate successful use of a PKI across multiple

Federal agencies operating within their own legally or institutionally mandated environments. Flexibility, adaptability, extensibility (ability to serve users having divergent environments and interests), expandability, scalability (ability to support a much larger user base), and, as is discussed below, interoperability, represent critical features which the technology and products must possess.

4.3 Support Multiple Technologies and Promote Interoperability

Industry has developed many different mechanisms for establishing a PKI. For example, several different encryption algorithms and digital signature schemes are in widespread use, both inside and outside of the government. Even when multiple vendors use the same basic technology, their implementations of the technology are not necessarily compatible or interoperable.

While the Steering Committee and other Federal policy-setting bodies aggressively promote compatibility and interoperability within the government infrastructure, the PKI must be flexible enough to accommodate a range of solutions for any given application, and to address the varying requirements and programmatic concerns of individual government agencies. Thus, pursuit of commonality and interoperability does not mean that the government must dictate a technical solution. In general, prescribing specific solutions would impede technological progress and constrain available business opportunities for commercial vendors. The viability and acceptability of commercially offered public key solutions will be market driven, allowing the PKI to be developed in response to government and commercial business needs.

Diversity in the use and selection of products, and interoperability, are critical.

4.4 Work Closely with Industry and Other Parties

Since the private sector will lead the development and implementation of security solutions, the Federal government must interact directly and continuously with private industry. We must articulate to industry our needs as a customer, reflecting an understanding of the commercial offerings and how commercially available information security technology and products can be applied. To promote these actions, the government will develop partnerships with interested commercial service and product providers.

Customers and users will have low tolerance for disconnected, piecemeal approaches. Accordingly, the primary focus in developing the PKI is to provide a robust overall infrastructure rather than one which supports single applications. Infrastructure development must take into account all existing and projected applications, not some subset.

Working closely with private companies in the Federal PKI efforts has been and remains a priority.

To those ends, the Steering Committee will maintain cognizance of the end-user applications and commercially available public key cryptographic products. The Steering Committee will ensure that both the requisite user and customer security products are considered and that infrastructure support services for those products exist. Further, where technology and implementation approaches allow, the Steering Committee will seek to foster long-term commonality among services, implementations, and interoperability among offered products. Finally, the Steering Committee will work to resolve all of the issues which may impede implementation of the PKI; several of these are set forth in Section 5 below.

SECTION 5. STRATEGY AND ACTIONS

Over the past two years, the Steering Committee has established pilot programs and projects to demonstrate aspects of the evolving PKI. It also established subordinate working groups to address specific areas of interest in the development of the PKI:

The Federal PKI Steering Committee focuses on three areas: technical matters, legal and policy issues, and agency business applications.

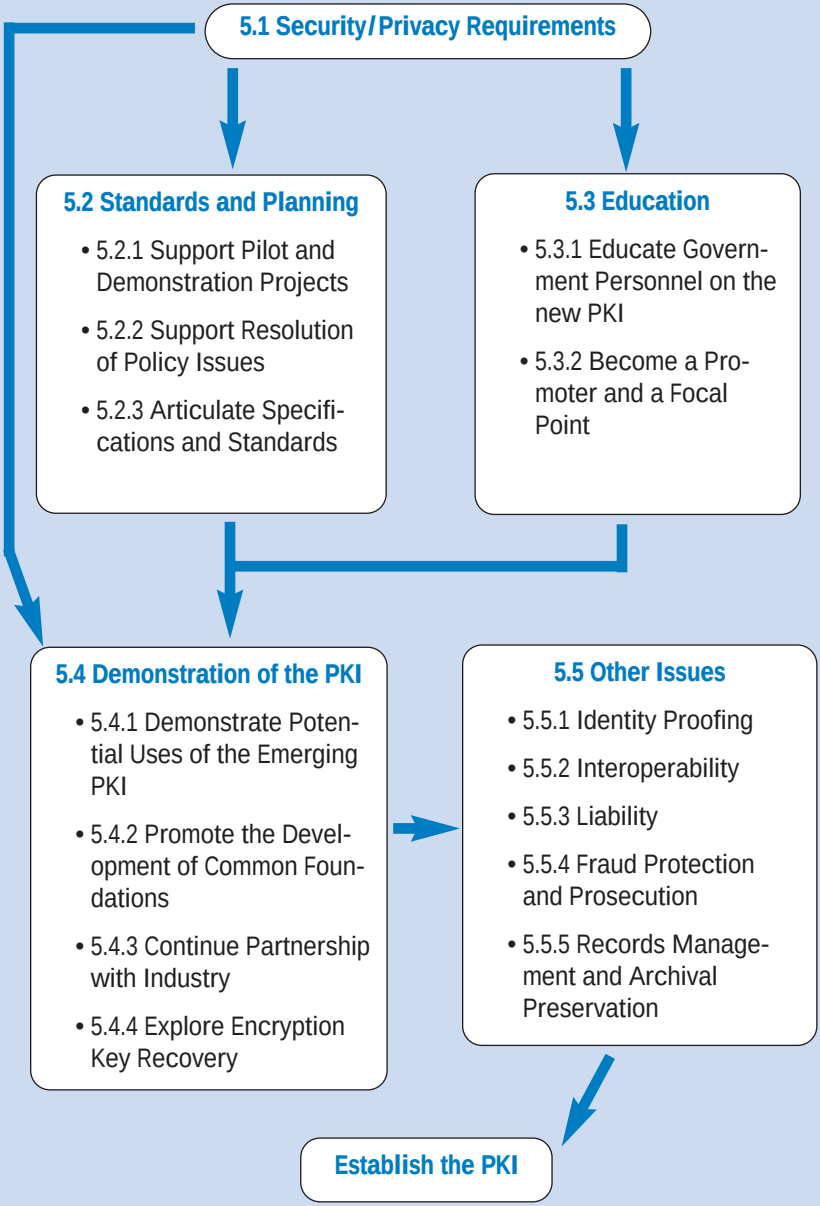
- The Business Working Group (BWG) which concentrates on identifying user requirements and applications that the PKI will need to support;
- The Technical Working Group (TWG) which addresses issues related to technology, specifications, standards, and interoperability; and
- The Legal and Policy Working Group (LPWG) which addresses policy, legal, and liability issues.

Members from each group work closely with commercial providers, agency representatives, other governments and advocacy groups to explore issues within its assigned domain. As necessary, each group refers technical or policy issues to the Steering Committee for resolution or assignment to another working group.

The working groups will identify activities to support development and implementation of the PKI. Lead agencies will be assigned which, with the support of other interested organizations, will be responsible for developing detailed plans and schedules to ensure completion of those assigned activities by established deadlines. These lead agencies may establish multi-agency groups as deemed necessary for the fulfillment of their assignments.

The Steering Committee has implemented an overall strategy, shown in Figure 5.1, to promote development and implementation of a robust PKI.

FIGURE 5.1 PKI STRATEGY/ACTIONS



5.1 Security/Privacy Requirements.

While each of the Steering Committee working groups plays a critical role in the development of the PKI, the Business Working Group (BWG) serves as the primary forum for summarizing the security and privacy requirements of the various Federal agencies and programs. In particular, the BWG is engaged in the following tasks:

- Identifying opportunities to transform how citizens interact with their government through electronic access to government services and information;
- Helping Federal agencies identify business opportunities (and the associated security and privacy requirements) for electronic access applications, including consultation with affected interest groups and other parties; and
- Providing a forum for the exchange of information on the PKI, security architecture, applications, products, interoperability, and various PKI pilot programs.

The starting place is defining agency business needs which may be fulfilled by a PKI-based solution.

Articulating requirements forms a useful framework for action, but it is not a one-time event. Requirements can be reevaluated and adjusted based on new information, experience with prototypes and pilot efforts, evolution of technology, and changes in business practices and the marketplace. The goal is not to solidify a fixed requirement or "specification" for the final PKI, but rather to ensure all user needs are being addressed as the infrastructure develops.

5.2 Standards and Planning

5.2.1 SUPPORT PILOT AND DEMONSTRATION PROJECTS. The Steering Committee plans to play a pivotal role in helping agencies deliver services electronically by sponsoring, supporting and encouraging pilot and demonstration projects. Appendix B identifies and discusses more than twenty projects which the Steering Committee has determined to be suited for this purpose. The Steering Committee will work closely with the Office of the Vice President, the National Partnership for Reinventing Government and Federal agencies and their partners in the major service-delivery demonstrations that are part of the *Access Amer-*

Agency pilot or demonstration efforts can provide good first steps.

ica plan. As agencies plan and implement these demonstrations of electronic delivery of government services, the Steering Committee will provide a focal point for problem-solving across agencies, and will serve as an advocate for common, interoperable security and privacy solutions.

5.2.2 SUPPORT RESOLUTION OF POLICY ISSUES. The Steering Committee is beginning to work more closely with other working groups, steering committees, and policy-making bodies, as appropriate, for resolution of critical policy issues needed to support the development of the PKI. There is growing agreement that most authentication and signature concerns can be addressed within the context of existing legal doctrine in conjunction with adequate audit and record-keeping controls. The Steering Committee is encouraging acceptance of digital signatures and electronic certificates by working closely with organizations, such as the American Bar Association and the American Bankers Association, and by developing a Model Certificate Policy for the Federal government.

Addressing and resolving policy issues must be done in cooperation with parties outside the Federal government.

5.2.3 ARTICULATE SPECIFICATIONS AND STANDARDS. The Steering Committee is fostering public/private partnerships to articulate appropriate specifications and standards. For example, under a Cooperative Research and Development Agreement (CRADA) sponsored by the National Institute for Standards and Technology (NIST), government and private industry representatives worked together successfully to identify minimum specifications for components of the PKI to promote their interoperability and to ensure a robust infrastructure design. The CRADA established a collegial working environment between government and industry necessary for the conduct of such complex technical work.

The Federal PKI architecture must be standards-based.

5.3 Education

5.3.1 EDUCATE GOVERNMENT PERSONNEL ON THE NEW PKI. The new PKI will be developed using advanced, state-of-the-art technology. It will almost certainly require reengineering business processes within each agency to realize fully the technology's promise of a transformed America. Because most of the underlying technology is new, few senior agency officials are familiar with it, or the benefits

it can provide. To support authorization and funding of pilot and demonstration programs, the Steering Committee serves to educate government officials on appropriate security and privacy technology, terminology, and benefits.

Those in agencies who deliver services must be made aware of the capabilities which a PKI provides for ensuring trusted electronic transactions.

5.3.2 BECOME A PROMOTER AND A FOCAL POINT. To date, the Steering Committee has been the focal point for coordinating and promoting the use of public key technology in Federal agencies. In the future, the Steering Committee will become the champion for the PKI, emphasizing long-term compatibility, commonality, and interoperability. The relevant security and privacy technologies will continue their rapid evolution. Unless the Steering Committee provides effective leadership, government efforts are likely to produce results counter to these objectives. For example, on-going government pilot programs are being managed by individual agencies, and absent the Steering Committee, there is no other interagency mechanism for coordination or communication of these efforts. In addition, many commercial vendors have become active in developing public key products, services, and security solutions that, for the most part, do not meet current government standards. There is insufficient industry movement to adhere to common specifications or to promote interoperability with competitors' products. A number of different key generation algorithms, digital signature methods, and infrastructure services are being marketed or developed, but even when they are based on the same underlying PKI technology, their implementations can be incompatible with each other.

The Federal PKI Steering Committee must promote fair and objective consideration by agencies of public key technology.

The Steering Committee believes that competition among commercial vendors is healthy and that attempts to restrain natural market forces can have unintended and undesirable effects. At the same time, the Steering Committee is working to achieve tighter coupling and better coordination of government activities. In particular, the Steering Committee hopes to act as a focal point with industry to promote interoperability by:

- Sponsoring, at periodic intervals, conferences among government participants aimed at ensuring that experience among Federal agencies is fully shared, and that common or at least compatible solutions are found;
- Participating in industry demonstrations, trade shows, conferences, and symposia;
- Promoting and facilitating continuing education and training in awareness of PKI technology and its applications; and
- Evaluating how commercial products may be assessed to determine their suitability for use within the PKI, and facilitating demonstrations of commercial products or services for a government audience.

5.4 Demonstration of the PKI

5.4.1 DEMONSTRATE POTENTIAL USES OF THE EMERGING PKI. Pilot programs and demonstrations can help define the PKI, not only in developing and implementing current state-of-the-art technology but in attempting to satisfy the business needs of each agency. Collectively, they constitute an important vehicle for getting feedback from users on operational and performance characteristics, and also for assessing subtle procedural and management issues.

To show that a PKI works, you must demonstrate it in real-life applications that touch people's lives in a positive way.

Information about each pilot is being used to evaluate contributions to the infrastructure from a technology or standards viewpoint. The information includes:

- The functionality and security services being implemented;
- The hardware and software being used;
- A description of whom the services support, the size of the user population, and their specific applications;
- The costs and benefits of the specific applications;
- The specific technology used for functions, such as traffic encryption, key exchange, signature, or hashing (i.e., the algorithms and key lengths, and any specific national or international standards that are being adopted);
- Contractor(s) involved;

- Schedule;
- Follow-on plans, such as expansion of functions, expansion of user base, or migration from "pilot" capability to a true operational status.

This information is also being used to assess common thrusts and directions among the efforts and to begin identifying core infrastructure requirements or services.

5.4.2 PROMOTE THE DEVELOPMENT OF COMMON FOUNDATIONS. To date, the PKI pilots and demonstrations have been separate, isolated, single-vendor initiatives. Three cross-cutting initiatives, described below, are planned or underway with the goal of relating the PKI pilots to current private sector efforts.

The first initiative is the Access Certificates for Electronic Services (ACES) Project, which is aimed at delivering public key certificates to the general public to facilitate secure access to government services. The goal of this project is to provide an expandable foundation to stimulate the widespread issuance of public key certificates and support the use of digital signatures as an authentication and document integrity technology. It is hoped that the ACES Project can be used to evaluate the adoption of a uniform and simple identity certificate, thus promoting interoperability among agency implementations.

The building blocks for a PKI must be carefully prepared, and pilot efforts must be woven together to make a cohesive whole.

The second initiative is to create a Federal Policy Management Authority (PMA) which would serve a policy-enabling function. In particular, the PMA would help each Federal agency desiring to use public key technology for an application to determine how to proceed thoughtfully and in a fashion which supports to the greatest extent reasonable and practical the goal of PKI interoperability. For example, the PMA would serve to help agencies create and implement uniform or consistent PKI policies and practices as set forth in instruments such as Certificate Policies, Certification Practice Statements (where the agency is running a Certification Authority), and concept of operations documents. The PMA may also oversee the function of a "Bridge CA" with which agencies can cause their CAs to interoperate, in the expectation that any CA which interoperates with such a "Bridge CA" will be able to interoperate with others that have done the same.

Led by the U.S. Department of Transportation, thirteen federal agencies have joined together to develop the third initiative, a comprehensive "Electronic Grants System" (EGS). This system, being pursued in concert with other efforts of the Interagency Electronic Grants Committee, will streamline the Federal grant process, improve efficiency and cut costs for grant customers (for example, by providing a common interface), and promote an interoperable PKI framework which benefits users and Federal agencies alike. A pilot EGS effort was featured in *Access America*. With funding from the Key Recovery Demonstration Project, secure features including digital signatures, encryption, and key recovery, have been added to the EGS pilot. This pilot is being tested with state government and university partners. Following completion of this testing, full EGS development can begin.

5.4.3 CONTINUE PARTNERSHIP WITH INDUSTRY. The Steering Committee intends to continue an open dialogue with a number of commercial entities (i.e., consultants, product developers, and service providers) about government requirements and industry products and standards. In most cases, discussions will occur without an established contractual relationship between the government and the vendor and without the immediate commitment of government funding. However, vehicles such as NIST's CRADA program will continue to be used to ensure formalized industry involvement in the development of the PKI. Through these informal and formal mechanisms, industry and government will continue to form a strong partnership and develop the PKI jointly.

We must proceed in close collaboration with private companies.

5.4.4 EXPLORING ENCRYPTION KEY RECOVERY. The Key Recovery Demonstration Project (KRDP) was initiated for the purpose of "demonstrating the practicability of a key recovery encryption regime as an element of a Key Management Infrastructure (KMI)/PKI." This effort involved keys used for data encryption, not those used for digital signatures, to avoid undermining non-repudiation and authentication. During 1997, thirteen government pilots demonstrated that key recovery can be successfully implemented in Federal government applications. Results gained from these pilots are currently being collected and analyzed with a final report expected by late 1998.

The Federal government will use feedback from these and future pilots, along with input from private industry and the American

public, to identify Federal key recovery needs. The government then will work with private industry to ensure that key recovery capabilities to support government needs are integrated into the PKI.

An agency must be able to recover the keys used for encryption purposes or else encrypted data could be irretrievably lost.

5.5 Other Issues

5.5.1 IDENTITY PROOFING. The Steering Committee must define a minimum set of standards for confirming the identity of a certificate holder ("identity proofing") in order to allow the certificate to be acceptable for use by Federal agencies. Such standards may involve requiring the holder to present himself or herself to the Certificate Authority with a photo identification or other proof that the person is who he or she claims to be.

As described above, a public key certificate "binds" an individual's public key to his or her identity. While robust identity proofing is important to the PKI, it takes on a different aspect for the Federal government because of concerns with protecting the privacy of government customers. Therefore, we must pay particular attention to the methods used to identify an individual and the process which supports that binding.

For a PKI to work, an individual's public key must be properly bound to that individual's identity.

A sufficiently robust identity proofing mechanism will, for example:

- Gather proofs of identity that can be linked to legacy databases to verify the existence of the individual;
- Incorporate methods to verify the identity being "proofed" belongs to the individual requesting the certificate;
- Cross-verify a set of data elements as part of the verification process; and
- Perform all of the functions in compliance with the Privacy Act.

In this vein, it should be emphasized that for many applications, identity-based authentication is not only unnecessary, it may be inappropriate. Agencies will need to consider carefully which applications require user authentication (e.g., to protect private infor-

mation). In many instances, such as downloading forms, anonymous transactions are appropriate.

5.5.2 INTEROPERABILITY. In order to maximize the possibilities for uniform access to government electronic services by the public and to support secure applications between and among different government agencies, the Steering Committee will emphasize the need for interoperability among the various agency pilots. Specifically, the Steering Committee has endorsed the Minimum Interoperability Specification for PKI Components (MISPC), that was jointly developed by NIST with leading PKI technology developers (see Section 6 below). The MISPC allows great flexibility for agencies because it specifies minimum interoperability, and describes the broad range of considerations to achieve that requirement (e.g. hierarchical and networked architectures, certificate format and certificate validation path protocols).

In general, agencies will be urged to follow two guiding principles: simplicity and modularity of design, so that the systems are extensible, providing the functionality desired by each group of users without unnecessary expense and effort. Since the public key infrastructure is evolving with changes in the market place, Federal system designs that incorporate these principles not only will be easier to build, but also easier to change. In order to provide further guidance in this important area, the Steering Committee will identify current open commercial standards that embody the above principles, and then publish its results on the gits.gov website.

Agency implementations of PKIs need to promote interoperability among those agencies.

5.5.3 LIABILITY. Deploying a comprehensive PKI will require agreement by all parties of an acceptable liability structure that balances the interests of users and service providers, particularly CAs, both governmental and non-governmental. Also required are the consumer protection standards to govern "retail" uses of the PKI. Recognizing that the Federal government already operates under legislation establishing its legal liabilities in many areas (for example, the Federal Tort Claims Act), the present common law, contract-based operating rules which govern the conduct of credit card issuers and banks inform the development of the PKI liability structure. Regulatory consumer protection standards, analogous to those that govern consumer use of credit and debit cards and checks, may ultimately be needed. Domestically, groups including the American Bar

Association and the National Automated Clearing House Association have begun examining these issues, and international organizations, such as the United Nations Commission on International Trade Law, have begun discussing them. National legislation in this area is premature since a broad-based consensus on the outlines of an appropriate liability structure has yet to emerge. The Federal government will be an active participant in developing this consensus.

Government liability for its actions, whether they involve a PKI or other mechanism, is established in law, but because the technology and its use are evolving, there is little case law available to guide the judiciary.

5.5.4 FRAUD PROTECTION AND PROSECUTION. Historically, for many government transactions, handwritten signatures and paper documents have been relied upon to establish the connection between an action and the individual and government entities who are parties to that action. There are concerns in the law enforcement community that PKI could weaken the government's ability to prosecute fraud successfully because of the absence of traditional pen-and-ink documentation. The Steering Committee will work to understand and address these concerns.

Use of public key technology is intended to reduce the potential for fraud, but there are law enforcement concerns which need to be identified and addressed if that goal is to be achieved.

5.5.5 RECORDS MANAGEMENT AND ARCHIVAL PRESERVATION. The National Archives and Records Administration (NARA) is responsible for storing important government information indefinitely for use by historians and other parties. Properly executing this responsibility creates several issues.

- Since the ability to decrypt encrypted information stored for an indefinite period is uncertain even if measures are taken to store the related keys (any defect in the key resulting from the passage of time could render the information unrecoverable), it is very unlikely that NARA will accept encrypted data for archival purposes.
- When NARA accepts records which are digitally signed, the certificate or some other information must uniquely link the digi-

Long-term management of records which have been signed or encrypted is a challenge that must be met for PKI use to be successful.

tal signature to an individual, position in government, and at a point in time, so that the context of the signed record is clear. This establishes what historians and archivists call "provenance."

Agencies other than NARA that maintain digital records for long periods of time must address similar concerns, including ensuring that encryption keys are preserved if encrypted records must be kept, and establishing and maintaining the provenance of digital signatures contained in records for legal or other purposes.

SECTION 6. ACCOMPLISHMENTS

Development of the PKI is well under way. The management structure identified in section 4 is implemented and functioning. The Steering Committee now comprises more than 50 agency representatives. The Steering Committee and its working groups meet monthly to address issues and to adopt various resolutions promoting the development of the PKI. For example, the Steering Committee adopted the PKI interoperability specification jointly developed by industry and government and identified in *Minimum Interoperability Specification for PKI Components (MISPC), Version 1*[3]. The Steering Committee has also adopted a resolution supporting the development and implementation of multiple CAs in the Federal government. The focus of these efforts is to ensure that the building blocks needed for a PKI are in place, and that Federal agencies are made aware of capabilities provided by the PKI so that they can make intelligent decisions on the use of public key technology to facilitate their internal operations and interactions with the public.

6.1 Federal PKI Outreach

The Steering Committee held a two-day meeting in May, 1997 that addressed various aspects of developing the PKI, such as procurement vehicles, budget options, state and local government partnerships, and business uses of the PKI technology. Results of this meeting have been incorporated into the Steering Committee's future planning activities, which can be found at gits-sec.treas.gov. Also available at that site is information describing the Steering Committee and each of the PKI pilots that are implementing the PKI technologies to solve a variety of business needs.

The Federal PKI Steering Committee and its Working Groups are reaching out to private companies, state governments, and other parties in developing an interoperable Federal PKI.

The Steering Committee has formed strong partnerships with numerous organizations involved in the PKI activities. Through NIST's CRADA

3. *Minimum Interoperability Specification for PKI Components (MISPC), Version 1*, (http://csrc.nist.gov/pki/) Output of NIST's Cooperative Research and Development Agreements for Public Key Infrastructure, June 5, 1997.

program, private industry has partnered with the Federal government to develop minimum interoperability specifications for the PKI components. The Steering Committee's Technical Working Group now has over 40 industry partner members helping to resolve the technical PKI issues. The Steering Committee is working with the American Bar Association, the American Bankers Association, and Congress to identify and resolve legal and policy issues that could impact the PKI. Finally, state and local governments, along with the European and Pacific Rim governments, are also working with the Steering Committee to ensure that the PKI is interoperable worldwide.

Thirteen PKI pilots, incorporating encryption key recovery functionality, were successfully demonstrated at the Key Recovery Demonstration Project Technology Conference held in November, 1997. Through the development of these pilots, optional key recovery services can now be included in the PKI.

6.2 Steering Committee's Working Groups

6.2.1 TECHNICAL WORKING GROUP (TWG)

- The TWG has produced a Certificate Profile for Federal Certificates that recommends the standardized certificate extensions that should be used in Federal certificates. This profile is closely coordinated with Internet, Multi-Level Information Systems Security Initiative (MISSI), the MISPC, and proposed banking profiles.
- The TWG has developed rules for encoding digital signature algorithm (DSA) keys and for using parameters and "inheriting" them in certificates and certification paths, that have been adopted in various standards documents.
- The TWG initiated early work in Technical Security Policies, that was a precursor to the now widely accepted PKIX 4 proposed standard outline of topics for Certificate Policies and Certification Practice Statements. While the overall focus of policy discussion has shifted to the Legal/Policy Working Group, the TWG continues to examine the technical component of certificate policies.

The Technical Working Group focuses on technology, hardware, and software issues.

- The TWG expects several digital signature algorithms to be used in the government and elsewhere. The TWG has developed an "end-systems" approach to interoperability in a multi-algorithm environment.

- The TWG has developed a Concept of Operations (CONOPS) document that describes a vision of an integrated Federal PKI. The CONOPS must evolve to adjust to developments in the commercial market. A revision to the CONOPS is planned that addresses interoperability in light of the following:
  - Current browser products implement a somewhat different PKI model than the "classical" hierarchical and network architectures, resulting in three fairly distinct PKI architectures now in use (hierarchical, network and "browser-style"). The TWG plans to address this in the CONOPS and provide recommendations for maximizing interoperability.
  - Another issue that the TWG plans to more fully develop in the CONOPS is certificate status validation and certificate revocation. This is a rapidly evolving area, and new standards for on-line certificate status validation are emerging. The TWG plans to extend the CONOPS to accommodate on-line certificate status validation.

6.2.2 BUSINESS WORKING GROUP (BWG)

- The BWG has expanded the Department of Transportation's Electronic Grants pilot to include requirements from other Federal agencies, state governments, and partners in academia.
- The BWG has hosted monthly meetings since October, 1996 to foster the exchange of information among Federal agencies about security technology and the security and information technology services provided by Federal agencies.
- The BWG has hosted a Security Requirements Workshop for the Department of Transportation Electronic Grants pilot, using this cross-agency pilot as a model for applications of Internet and security technology, which can address the needs of multiple agencies and simplify customer interactions with the Federal government.

The Business Working Group focuses on agency applications.

- The BWG has hosted educational presentations by contractors on elliptic curve cryptography and cost models for the PKI.

6.2.3 LEGAL AND POLICY WORKING GROUP (LPWG)

- The LPWG has provided a forum for discussion of legal and policy issues that have impeded progress within the Federal government with respect to adoption of public key technology.
- With a primary focus on digital signature, the LPWG has provided constructive critiques of both an Internet Engineering Task Force draft certificate policy framework and the Request for Comment published by the Administrative Office of the U.S. Courts.
- The LPWG has had extensive discussions of risk management issues facing CAs which led to the formulation of a new business model for issuing certificates that was adopted by the General Services Administration (GSA) for use in their ACES initiative.
- The LPWG is currently overseeing the production of a model Federal Certificate Policy Statement.

The Legal and Policy Working Group focuses on legal and policy matters.

Section 7. Membership of the Federal Public Key Infrastructure Steering Committee

Current membership list can be found at gits-sec.treas.gov

Organization	Point of Contact	Email Address
Treasury	Richard A Guida, P.E. (Chair, FPKI Steering Committee)	Richard.Guida@cio.treas.gov
OMB	Bruce McConnell	mcconnell_b@a1.eop.gov
OMB	Peter Weiss	Peter_N._Weiss@omb.eop.gov
NPR	Andy Boots	andy.boots@npr.gov
Army	Gary Robison	robisga@hqda.army.mil
BLS	Elaine Chen-Nash	chen-nash_e@bls.gov
BLS	Arnold Bresnick	bresnick_a@bls.gov
DEA	Felix DeMicco	(headquarters)
DOD	Karen Gorsuch	karen.gorsuch@osd.pentagon.mil
DOD	Paul Grant	paul.grant@gsa.gov
DoED	John Tressler	john_tressler@ed.gov
DOE	Tom Rowlett	thomas.rowlett@hq.doe.gov
DOE	Sharon Shank	sharon.shank@hq.doe.gov
DOI	John Haines	jhaines@ios.doi.gov
DOJ	Jerry Ormaner	ormanerj@justice.usdoj.gov
DOJ	Susan Koeppen	skoeppen@leo.gov
DOJ	John Lynch Jr.	jlynchjr@leo.gov
DOT/FRA	Brad Smith	bradley.smith@fra.dot.gov
DOT	Ann Fisher	ann.fisher@ost.dot.gov
EPA	William Gill	gill.william@epamail.epa.gov
EPA	Kimberly Nelson	nelson.kimberly@epmail.epa.gov
FDIC	Garret Mussmann	Gmussmann@fdic.gov
GSA	Judith Spencer	judith.spencer@gsa.gov
GSA	Allen Church, PhD	allen.church@gsa.gov
IRS	Stephen H Holden, PhD	Stephen.H.Holden@ccmail.irs.gov
NIH/DHHS	Peter Alterman, PhD	peter_alterman@nih.gov
NARA	William Lefurgy	william.lefurgy@arch2.nara.gov

Organization	Point of Contact	Email Address
NARA	Mark Giguere	mark.giguere@arch2.nara.gov
NARA	Mary Donovan	mary.donovan@arch2.nara.gov
NASA	James Radosevich	james.radosevich@hq.nasa.gov
NASA	Yuan-Kwei Liu	ykliu@mail.arc.nasa.gov
NASA - ARC	Tice F DeYoung	tdeyoung@mail.arc.nas.gov
NIST	Miles Smid	miles.smid@nist.gov
NIST	Bill Burr	william.burr@nist.gov
NIST	Donna Dodson	donna.dodson@nist.gov
NIST/FNC	Dennis Steinauer	dds@nist.gov
NRC	Louis H Grosman	lhg@nrc.gov
NSA	Patty Moreno	plmoren@missi.ncsc.mil
NSA	Suzanne Brandon	scbrand@missi.ncsc.mil
NSF	Gerald B Stuck	gstuck@nsf.gov
NTIS	Keren Cummins	kcummins@fedworld.gov
NTIS	Bill Donovan	bdonovan@apollo.fedworld.gov
NTIS	Mike Williams	mwilliams@fedworld.gov
PTO	Arthur Purcell	purcell@uspto.gov
SBA	Donna Clark	donna.clark@sba.gov
SBA	Howard Bolden	howard.bolden@sba.gov
SSA	Sara Hamer	sara.hamer@ssa.gov
SSA	John Sabo	john.t.sabo@ssa.gov
SSA	Bob Daniels	bob.daniels@ssa.gov
Treasury	Gary Garner	gary.garner@fms.sprint.com
Treasury/FMS	Calvin Kidd	calvin.kidd@fms.sprint.com
Treasury/FMS	John Moore	john.moore@fms.sprint.com
USDA	Kelvin O Fairfax	kelvin_fairfax@fcs.usda.gov
USDA (NFC)	Kathy Sharp	kathy.sharp@usda.gov
VA	Dan Maloney	maloney.dan@forum.va.gov
VA	Cathie Ward	cathie.ward@mail.va.gov

Section 8. List of Acronyms

Acronym	Meaning
ACES	Access Certificates for Electronic Services
AIS	Automated Information System
ARC	Ames Research Center
ARL	Army Research Lab
ARPA	Advanced Research Projects Agency
ATM	Automated Teller Machine
AWR	Annual Wage Reporting
BAA	Broad Agency Announcement
BWG	Business Working Group
CA	Certification Authority
CAW	Certification Authority Workstation
CITAC	Computer Investigations and Infrastructure Threat Assessment Center (now called the National Infrastructure Protection Center)
CKL	Compromised Key List
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRADA	Cooperative Research And Development Agreement
CRL	Certificate Revocation List
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DII	Defense Information Infrastructure
DOD	Department of Defense
DOE	Department of Energy
DoEd	Department of Education
DOJ	Department of Justice

Acronym	Meaning
DOT	Department of Transportation
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTS	Defense Travel System
EBT	Electronic Benefit Transfer
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
EPA	Environmental Protection Agency
EPAFS	Electronic Patent Application Filing System
ERA	Electronic Research Administration
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCS	Food and Consumer Services
FHA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FNCAC	Federal Networking Council Advisory Committee
FTA	Federal Transit Authority
GITS	Government Information Technology Services Board
GSA	General Services Administration
IETF	Internet Engineering Task Force
IRS	Internal Revenue Service
ISOC	Internet Society
KMI	Key Management Infrastructure
KRDP	Key Recovery Demonstration Project
LAN	Local Area Network
LLNL	Lawrence Livermore National Laboratory
LPWG	Legal and Policy Working Group
MISPC	Minimum Interoperability Specification for PKI Components
MISSI	Multi-Level Information Systems Security Initiative
NAFTA	North American Free Trade Agreement

Acronym	Meaning
NASA	National Aeronautics and Space Administration
NATAP	North American Trade Automation Prototype
NCS	National Communications System
NCSC	National Computer Security Center
NFC	National Finance Center
NIH	National Institutes of Health
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NPR	National Performance Review; now National Partnership for Reinventing Government
NRC	Nuclear Regulatory Commission, or National Research Council
NSA	National Security Agency
NSF	National Science Foundation
NTIS	National Technical Information Service
PMA	Policy Management Authority
PEBES	Personal Earnings and Benefit Estimate Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Proof-of-Concept
SBA	Small Business Administration
SBU	Sensitive but unclassified
SDSI	Simple Distributed Security Infrastructure
SPKI	Simple Public Key Infrastructure
SPS	Standard Procurement System
SSA	Social Security Administration
SSL	Secure Socket Layer protocol
TSP	Trade Software Package
TWG	Technical Working Group
UN/EDIFACT	United Nations/EDI for Financial, Accounting, Commerce, and Transport
USDA	United States Department of Agriculture

Acronym	Meaning
USPTO	United States Patent and Trademark Office
WIPO	World Intellectual Property Office
WWW	World Wide Web

APPENDIX A. ESSENTIAL PKI MANAGEMENT FUNCTIONS

The following lists the minimum essential functions the PKI needs to provide.

- Generating and certifying public and private keys, and disseminating and managing public key certificates to support networked applications in the areas of identification, authentication, non-repudiation, and confidentiality;
- Cross-certifying certificates within the infrastructure and with other infrastructures;
- Maintaining repositories that make certificates and information about the status of certificates available;
- Providing standards for key exchange (algorithms, protocols, and formats);
- Providing for key recovery (for encryption keys only);
- Ensuring the current validity status of keys (e.g., generating and distributing Compromised Key Lists (CKL) and Certificate Revocation Lists (CRL), and providing a process and mechanism for managing those lists);
- Creating and supporting a secure delivery service for keys;
- Accounting and auditing security and business-relevant events;
- Performing overall day-to-day operation, administration, management, and logistics support for the FPKI.

The Federal Policy Management Authority will supply overall security policy and guidance concerning PKI matters.

APPENDIX B. OVERVIEW OF THE PKI PILOT PROJECTS

The PKI pilot projects performed by each Federal agency and discussed in *Access with Trust* are described below. Several of the projects entailed demonstrating the use of key recovery for encryption keys. For that purpose, the National Institute of Standards and Technology (NIST) provided technical support, which included issuing a Broad Agency Announcement (BAA) soliciting information from vendors about the availability of products, components, and services that could be used for key recovery. NIST then assisted the pilot agencies in the development of their implementation plans and key recovery procedures, and acted as the technical lead for the testing of the pilot key recovery systems. NIST coordinated the development of comprehensive test suites for the pilot systems and assisted in evaluating and reporting the test results. NIST also procured a CA and is performing experiments to determine the extent to which a root CA service can be provided to the other pilots.

Each of the pilot projects was important and significant in its own way, so the order in which they are listed below (alphabetically by cabinet agency, then by other agency or organization) does not connote significance.

1. DEPARTMENT OF AGRICULTURE / FOOD AND CONSUMER SERVICES

Electronic Benefits Transfer. In an initiative to employ security technologies in the Electronic Benefits Transfer (EBT), the United States Department of Agriculture's Food and Consumer Services (FCS) is piloting a security system. After a successful demonstration, FCS has made provisions to pilot the demonstrated technologies in a live EBT environment. This will be accomplished by selecting states in which the security technology will be integrated into operational EBT systems.

2. DEPARTMENT OF AGRICULTURE/NATIONAL FINANCE CENTER

Trusted Certification Authority at the National Finance Center. This project focuses on the requirements and functions necessary to allow the National Finance Center (NFC) to support digital signature requirements from client agencies and to have the NFC's CA participate in interoperability testing with NIST as a trusted CA site using COTS software. Selected application documents, that are electronically submitted and require

an original signature, are transmitted to NFC with an attached digital signature. The digital signature is stored with pertinent document information prior to application processing. Along with this initial pilot, NFC is establishing Internet Protocol Security Encryption with Virtual Private Network technology using certificates with various applications at NFC. NFC has begun interoperability testing with NIST. Further interoperability testing with NIST and other designated agencies will be conducted. Hardware, software, and cryptographic modules upgrades and enhancements will be implemented to ensure that NFC's goal of offering a CA that complies with FIPS 140-1 Security Level III requirements is realized.

3. DEPARTMENT OF COMMERCE/NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Purchase Order Request System. The Information Technology Laboratory at the NIST has been focusing on the design, implementation and use of advanced systems for cryptographic based computer security and office automation systems. The Purchase Order Request System combines both technologies into a system which will provide NIST with basic infrastructure components necessary for migration into a paperless process. The system allows users to generate and digitally sign purchase order requests, which are then routed to an approving authority. The approving authority reviews the request, verifies the user's signature and, if in agreement with the request, signs it and sends the electronic form to the administrative officer for processing. The system has been developed in a modular fashion so that both the digital signature module and the certificate management module can be used to support other applications using digital signature technology.

4. DEPARTMENT OF COMMERCE/NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Root Certification Authority Reference Implementation. The purpose of this project is to develop an initial implementation of a top level or root CA for the PKI and to conduct experiments with Federal agencies who are actively engaged in the development and use of digital signature technology. The CA will issue certificates to various pilot CA applications now being developed by Federal agencies. This test will foster a flexible hierarchy, which could support agency-level digital signature based applications. The initial root CA will also be used to cross-certify with CAs operated or provided by commercial vendors.

5 DEPARTMENT OF COMMERCE / NATIONAL TECHNICAL INFORMATION SERVICE

Secure Web and Certification Authority. The NTIS FedWorld Secure Web and CA Project has prototyped trusted-agent services that support digital signature, encryption of files and messaging, and authorized emergency access to encrypted information through key recovery management. NTIS currently provides the security infrastructure supporting the DOT Electronic Grants System and the NIH Electronic Grants Pilot, both detailed below, and is actively exploring partnerships with other agencies that need digital signature and encryption capabilities incorporated into current or planned web-based applications.

6. DEPARTMENT OF COMMERCE / PATENT AND TRADEMARK OFFICE

International Patent Document Exchange Project. The USPTO International Patent Document Exchange Project will demonstrate the exchange of patent documents in secure electronic form between the Trilateral Offices (USPTO, European Patent Office, and Japanese Patent Office) and the International Bureau of the World Intellectual Property Office (WIPO) to reduce processing costs and the burden on applicants. The pilot implements encrypted e-mail with a key recovery capability.

7. DEPARTMENT OF COMMERCE / PATENT AND TRADEMARK OFFICE

Electronic Patent Application Filing System (EPAFS). The EPAFS was started as a project designed to help determine the feasibility of using the Internet and the WWW as a platform for electronic filing of patent applications. The development of EPAFS was initially focused on the filing of applications under the Patent Cooperation Treaty, a format that has international applicability. Currently, extensions and enhancements are being made to EPAFS for demonstration in conjunction with the participation of the USPTO in the KRDP under sponsorship of the GITS Board. Recent developments in the areas of high-grade encryption and digital signature technology coupled with emerging vendor products and software components offer promising solutions to many of the problems associated with moving to an electronic patent filing and processing environment. For example, encryption key recovery interchange standards and software modules will now support and enhance the recovery capabilities of archival data and other information assets. General business practices will be enhanced with this new key recovery capability. The USPTO will now be able to concentrate efforts on delivering better services to the Intellectual Property (IP) practition-

ers and general IP community now that certain security requirements such as data archival/retrieval, strong encryption, and nonrepudiation can be met with commercially available key recovery and digital signature products and service offerings.

8. DEPARTMENT OF DEFENSE / DEFENSE INFORMATION SYSTEMS AGENCY

Defense Travel System. The Defense Travel System (DTS) will provide the means for identifying and authorizing travel needs, estimating the cost of each trip, arranging for transportation and ticketing, ascertaining whether housing and dining facilities are available during business travel, paying transportation bills, performing checkbook functions, reimbursing travelers, and making financial settlement for each trip. To support digital signature, the Department of Defense (DOD) Public Key Infrastructure will provide the means for DTS users to acquire medium assurance digital signature certificates and provide access to those certificates.

9. DEPARTMENT OF DEFENSE / DEFENSE LOGISTICS AGENCY

Standard Procurement System. The Standard Procurement System (SPS) will provide a single DOD procurement system with electronic commerce capability. The SPS is a COTS application based upon a relational database application that has been evaluated by the National Computer Security Center (NCSC). The SPS will process only sensitive but unclassified (SBU) information, financial data, trade secrets, technical methods, and other proprietary information as well as source selection data. The business goals of the SPS include meeting procurement functional requirements, accepting and outputting standard DOD data elements, and reducing operating expenses of the DOD procurement infrastructure.

10. DEPARTMENT OF DEFENSE / NATIONAL SECURITY AGENCY

Multi-level Information Systems Security Initiative. The Multi-level Information Systems Security Initiative (MISSI) is a network of security initiatives employing a framework for the development and evolution of network system security solutions. These solutions draw on interoperable, complementary COTS and government-sponsored security products and standards to provide flexible, modular security for networked information systems across the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII).

The underlying Network Security Framework, developed in

partnership with customers and technology suppliers, addresses security services. It includes identification and authentication, integrity, non-repudiation, confidentiality, and availability. Each of the framework solutions, which provide these services, includes requirements for a supporting network security infrastructure.

Within the Network Security Framework, NSA is analyzing the commercial PKI products and services to determine requisite characteristics and the state of the commercial technology in order to make recommendations regarding the use of these industry offerings. To support near-term DOD customers and gain technology expertise, the PKI functions have been implemented through a government-sponsored CA Workstation (CAW) that manages keys, privileges, and certificates. The current operational MISSI CAW hierarchy focuses on supporting FORTEZZA® Crypto Cards.

In the near term, the Defense Information Systems Agency (DISA) and NSA as part of MISSI are utilizing the CAW and FORTEZZA® Crypto cards to field a high assurance PKI for the Defense Messaging System (DMS) for organizational messaging traffic. This implementation supports the required DMS user security services through the use of the FORTEZZA® Crypto card and an X.500 directory.

A long-term goal of MISSI is to support customer PKI needs, through a combination of (1) acting as an unbiased authority validating the security goodness of the commercial PKI products/services, and (2) driving the development of robust PKI solutions by specifying requirements and transferring technology expertise to industry.

11. DEPARTMENT OF ENERGY

Electronic Research Administration Demonstration. This project will test emerging security technologies for EDI that are based on the Internet standards for secure e-mail. Six Federal agencies and eight academic research organizations currently involved in Electronic Research Administration (ERA) will participate in this project. This project will test the interoperability of multiple vendors' products across an open systems environment. The initial implementation will focus on processing encrypted electronic grant applications and providing key recovery services.

12. DEPARTMENT OF ENERGY / LAWRENCE LIVERMORE NATIONAL LABORATORY

Badges and Security Clearances. This project uses the PKI digital signature capability to sign and route, via E-mail, an electronic form used to request changes in clearance/badge status. The form originates in the Lawrence Livermore National Laboratory's (LLNL's) Human Resources Department and is routed to the Security Department. Human Resources signs and Security verifies the form.

13. DEPARTMENT OF ENERGY / LAWRENCE LIVERMORE NATIONAL LABORATORY

Public Key Infrastructure. The LLNL is in the process of building the PKI to support both its programmatic and business operations. Part of these operations include network interactions with many other DOE laboratories, facilities, and vendors. In order to utilize the network, LLNL's infrastructure must provide strong authentication, nonrepudiation, message integrity, and privacy for the information being exchanged. An emergency access capability is viewed as a critical part of this infrastructure if the full potential of public key encryption technology for privacy is to be realized. LLNL will exercise the key recovery capabilities of a commercial software product to ascertain its ability to meet requirements.

14. DEPARTMENT OF THE TREASURY

Secure Electronic Messaging System. The U.S. Department of Treasury's Office of Corporate Systems Management (OCSM) has implemented a pilot project aimed at exploring the use of PKI tools to facilitate the flow of procurement information. Specifically, the project is designed to reduce the time and resources needed to request, review, and approve task orders issued under existing contracts. In the case of this pilot, OCSM has instituted a system that enables Treasury employees to interact securely with key employees of a Treasury contractor over the Internet. Encryption, digital signatures, and key recovery functionality are being used to secure all transactions.

15. DEPARTMENT OF THE TREASURY / U.S. CUSTOMS SERVICE

North American Trade Automation Prototype. Article 512 of the North American Free Trade Agreement (NAFTA) states that, to the extent possible, the three Parties (United States, Canada, and Mexico) will agree, for the purpose of facilitating trade, to harmonize documentation, standardize data elements, and

accept an international data syntax for the exchange of information. The desired effect of these measures is to streamline the clearance of commercial goods through the customs processes of the respective Parties.

To meet these requirements, the NAFTA partners have implemented a prototype electronic commerce initiative that is intended to demonstrate how the NAFTA customs and trade processes could function in a cost effective, secure manner. Designated as the North American Trade Automation Prototype (NATAP), the initiative includes live operations at U.S., Mexican, and Canadian frontiers. While the prototype is low volume relative to the daily cross-border activities, it has been implemented by over 400 trade partners in North America, and therefore represents a unique exploration of state of the art technology by government and commercial organizations.

Through NATAP, government and commercial organizations have the opportunity to exercise a business-driven application of electronic commerce over the Internet and to validate the use of standardized international trade data elements. Further, since the application has been implemented using the Internet, it has been designed with a high level of security features to ensure confidentiality and authenticity of business sensitive information contained in routine customs declarations, while preserving the availability of that information through key recovery.

16. DEPARTMENT OF TRANSPORTATION / FEDERAL RAILROAD ADMINISTRATION

U. S. Electronic Grants. Led by the U.S. Department of Transportation, thirteen Federal agencies (Departments of Education, Energy, Interior, Labor, Environmental Protection Agency, General Services Administration, Office of Naval Research, Small Business Administration, Federal Railroad Administration, Federal Transit Administration, Federal Aviation Administration, Federal Highway Administration, and U.S. Coast Guard) have joined together to develop a comprehensive "Electronic Grants System" (EGS). This system will streamline the Federal grant process, improve efficiency and cut costs for grant customers and federal agencies. EGS uses Java and Information Broker technologies to enable any grant customer to electronically exchange grant data with any Federal agency, or multiple agencies, using a single WWW user interface. These technologies also provide a truly interactive user interface by transmitting grant data to and from

Federal databases in near real-time. In addition, the EGS facilitates government-wide information sharing by maintaining a standard data structure based on existing EDI transaction sets. An EGS "proof of concept" module was developed with funding from the NPR and its Government Information Technology Services (GITS) Board Innovation Fund. After extensive agency and customer testing, the pilot has demonstrated the effectiveness of the system concept. Following this success, the project was featured in *Access America*, the Vice-President's report.

With funding from the GITS Board's Key Recovery Demonstration Project, secure features including digital signatures, encryption and key recovery, have been added to the EGS pilot. This secure pilot is currently being tested with state government and university partners. Following completion of this testing, full EGS development will begin.

17. FEDERAL BUREAU OF INVESTIGATION (FBI)

Internet Communications Security. This project is to develop a method for the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) to communicate with representatives of private industry, the academic community, and other law enforcement agencies in a secure manner, while at the same time supporting key recovery. The pilot will test secure E-mail over the Internet and will involve security services such as digital signature and encryption.

18. FEDERAL BUREAU OF INVESTIGATION

Secure E-mail. This project is to secure the contents of E-mail messages sent within the Federal Bureau of Investigation (FBI) and between the FBI and other Department of Justice (DOJ) components. This project focuses on a small number of e-mail users to demonstrate the use of encryption for confidentiality and the feasibility of providing key recovery for the e-mail messages.

19. FEDERAL NETWORKING COUNCIL / NATIONAL SCIENCE FOUNDATION

Collaborations in Internet Security. This project is aimed at promoting multi-agency collaborations in the security arena. Eight agencies are participating directly (i.e., DOE, DOD/Army Research Lab (ARL),Advanced Research Projects Agency (ARPA), National Institutes of Health (NIH), National Communications System (NCS), NIST, National Science Foundation (NSF), and

National Aeronautics and Space Administration (NASA)). Other Federal entities will be engaged indirectly through the Federal Networking Council (FNC) outreach efforts. Participation in this pilot effort will be open to the academic and private sectors (both software and hardware vendors), including members of various communities such as the Internet Society (ISOC), the Internet Engineering Task Force (IETF), and the Federal Networking Council Advisory Committee (FNCAC). The governing principles behind the Security Testbeds include employment of an open process (with the activities and results open to participation and comment by both public and private sector participants); a focus on multi-vendor technologies; an emphasis on testing and experimentally deploying security technologies emerging from research and private sectors as well as security technologies currently in use in the commercial environment; and an underlying objective to ensure interoperability among the broad Internet community (i.e., Federal, private, and academic).

This effort will also include development of a laboratory accreditation program for testing and certifying Internet security software and systems. This process will be modeled on NIST's National Voluntary Laboratory Accreditation Program, which tests and accredits systems and products for Federal and private sector users. The FNC is tasked with bridging the gap between the advanced networking technologies being developed by research FNC agencies and the ultimate acquisition of mature versions of these technologies from the commercial sector.

20. GENERAL SERVICES ADMINISTRATION

Paperless Federal Transactions for the Public. The Paperless Federal Transactions for the Public pilot was an early attempt to develop a user friendly, interoperable solution utilizing Federal and industry standards, where available, to provide a public key architecture that would satisfy the concerns of the regulatory agencies for performing electronic commerce and funds transfer over the worldwide web. By developing partnerships with industry and concentrating on COTS products, a proof-of-concept pilot was designed and implemented using public key technology to enable digital signature and encryption. The concept called for a "plug-and-play" architecture requiring industry partners to adhere to a set of Federal standards, including the use of the DES encryption algorithm, and DSS for digital signatures. Six agencies agreed to participate and develop applications for use with the Paperless pilot. Each was provided a web server, server

software, client software, and hardware tokens containing their key pairs.

The pilot completed its first successful implementation when the GSA FTS2001 procurement was conducted in a completely paperless environment. The Request for Proposals was released on the Internet digitally signed in a downloadable format with attendant software for verifying the signature. Potential offerors were then issued hardware tokens containing digital signature key pairs which were used to sign their electronic submissions. For this procurement, no paper submissions were required saving approximately $1.5 million in government resources which would otherwise have been expended in handling paper submissions.

21. NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Public Key Infrastructure. The PKI pilot project will investigate (1) the use of standard X.509 certificates for public key infrastructure, (2) the deployment issues related to the PKI, and (3) other key infrastructure, such as Simple Public Key Infrastructure/Simple Distributed Security Infrastructure (SPKI/SDSI).

The study of the PKI includes the COTS implementation of the PKI technology. The deployment issues related to the PKI (i.e., scalability, reliability, performance, maintainability, and cost) will be investigated. Additionally, the Ames Research Center (ARC) will study the latest trend in the area of the PKI, such as SPKI/SDSI. The study of SPKI/SDSI covers the research cooperation between ARC and MIT. SPKI/SDSI emphasizes unique approaches to naming and delegation of authority. It will be useful for authorization and access-control applications. A SPKI/SDSI version 2.0 prototype is being implemented at MIT.

22. NATIONAL INSTITUTES OF HEALTH

Electronic Research Administration/Public-Key Infrastructure. All secure systems require that trust be established between system users. This concept is embodied in the Electronic Research Administration (ERA)/Public Key Infrastructure (PKI) pilot deployed by the National Institutes of Health (NIH). The NIH pilot enables grantee organizations to exchange data with NIH in a trusted manner.

Many grantee organizations participating in the pilot with NIH have implemented grant administration systems. These systems

are capable of generating grant administration data in a standard encoded format (e.g., EDI). The NIH pilot provides these organizations with a non-proprietary means to submit the encoded data securely to NIH.

More specifically, the NIH pilot demonstrates how World Wide Web (WWW), Electronic Data Interchange (EDI), and PKI technologies can be integrated to create a secure electronic grants system. For PKI services NIH has partnered with the National Technical Information Service (NTIS). NTIS received funding from the Government Information Technology Services Board (GITSB) Key Recovery Demonstration Project to prototype Certification Authority (CA) and Key Recovery Agent (KRA) functions for the NIH pilot.

As part of its PKI service, NTIS has supplied a workgroup security tool to NIH pilot participants (i.e., grantee organizations). Using this GUI-based tool, grantees can digitally sign files (e.g., EDI transactions containing grant applications). These files can then be uploaded to NIH via a Secure Socket Layer (SSL) channel. Additionally, grantees can use the tool to encrypt data on their local systems.

The NIH pilot is part of an overall NIH effort to work with other Federal agencies and the research community to develop an electronic research administration system that promotes standardization of data and flexibility in non-proprietary technological solutions.

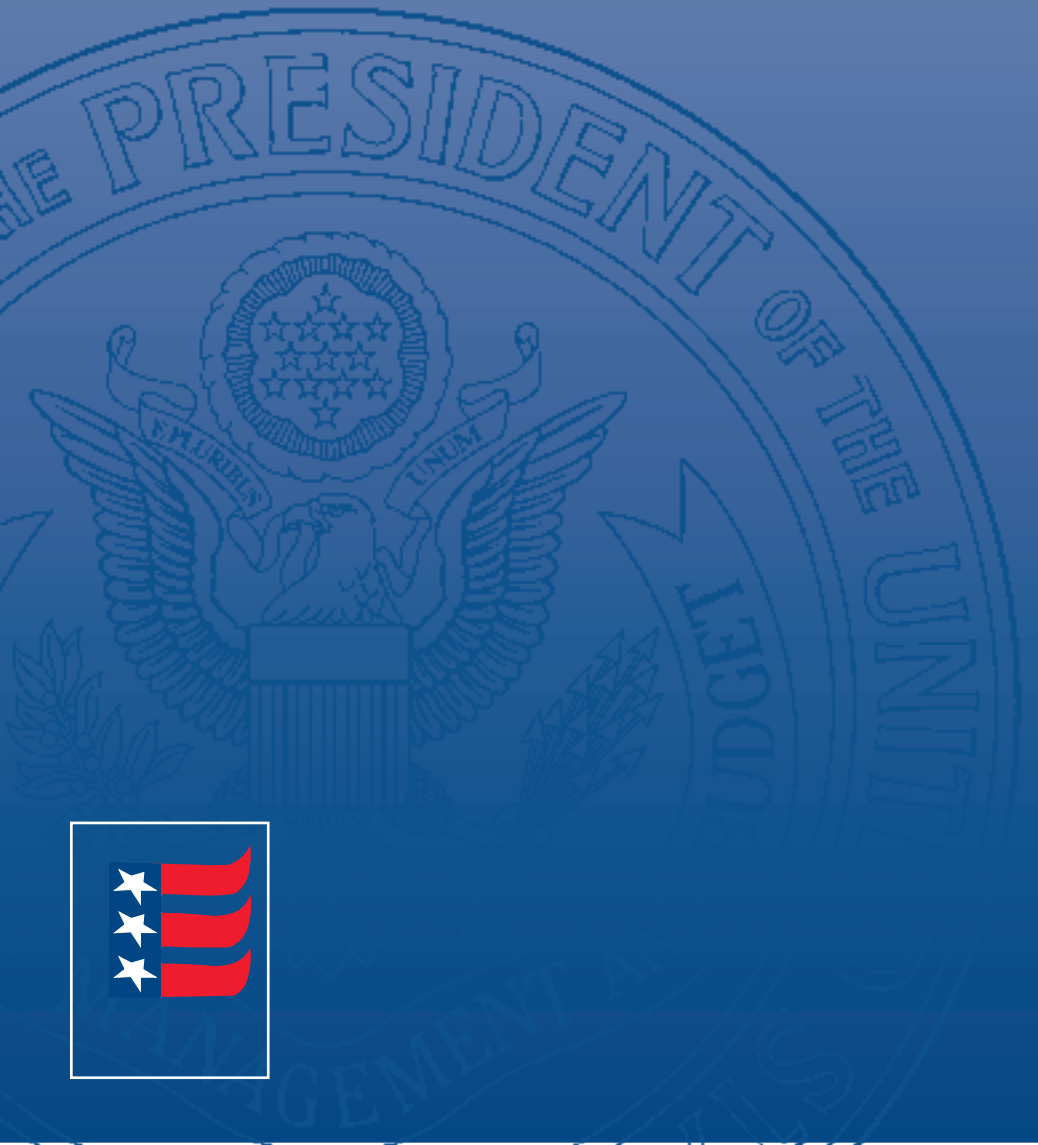
23. SMALL BUSINESS ADMINISTRATION

Electronic Lending Program. The SBA Electronic Lending Program is an initiative to re-engineer business loan guarantee processes. The Key Recovery Project will feature acceptance of electronic applications for SBA guarantees on FA$TRAK loans from a small group of bank lenders.

24. SOCIAL SECURITY ADMINISTRATION

Annual Wage Reporting (AWR) Pilot. SSA is responsible for processing the data from approximately 220,000,000 W-2 and W-3 forms each year. Approximately 10,000,000 of these forms are submitted by employers who have 15 or fewer employees. The vast majority of these submissions are on paper and require significant manual processing by SSA before the data is usable by SSA or the Internal Revenue Service (IRS). In an effort to streamline this process, SSA entered into a proof-of-concept (POC)

demonstration project with Pitney Bowes, Inc. to test the usefulness of the Internet as a means for small businesses to submit their W-2 and W-3 data to SSA. The POC demonstrated that a trusted third party such as Pitney Bowes could work closely with SSA on an ongoing workload without compromising the privacy or security of the information that SSA is charged with processing, and that data can be moved over open networks while employing encryption and other data security technologies. The pilot was an important opportunity to learn more about our customers, third parties providing secure authentication and certification services, the PKI, key recovery services, systems issues related to the PKI and the Internet, and how such services should be marketed.


PRESIDENT OF THE UNITED
E PLURIBUS
UNUM