CIO PKI/SMART CARD PROJECT

APPROACH FOR BUSINESS CASE ANALYSIS OF USING PKI ON SMART CARDS FOR GOVERNMENTWIDE APPLICATIONS

FINAL DELIVERABLE #0003

General Services Administration

Order # T-03-00DS-F002
Contract # GS00T97NSD0023

Washington, DC

Presented to CIO Council 18 April 2001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12/1/2000	Report 12/1/2000

4. TITLE AND SUBTITLE
CIO PKI/Smart Card Project Approach for Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications Final Deliverable #0003

5. FUNDING NUMBERS

6. AUTHOR(S)
Unknown

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

General Services Administration
Washington DC

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Booz·Allen & Hamilton, under contract to the General Services Administration, was tasked to document a business case approach that can be utilized by Federal agencies considering an investment in Public Key Infrastructure (PKI) on smart cards for governmentwide applications. The Chief Information Officer (CIO) Enterprise Interoperability Emerging IT Committee plans to use the methodology presented herein to help these agencies build business cases that examine using smart cards in concert with the emerging Federal PKI to provide Government employees with a standard identification card to be used for authentication, access control, and electronic commerce (e-commerce). The intended audience of this report is investment decision makers of Federal agencies that are seeking information assurance solutions for their agencies and those practitioners charged with developing business cases.

14. SUBJECT TERMS
IATAC Collection, smartcards, public key infrastructure, cryptographic smart cards, information assurance, nonrepudiation, authentication, data integrity, confidentiality

15. NUMBER OF PAGES
86

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Booz·Allen & Hamilton, under contract to the General Services Administration, was tasked to document a business case approach that can be utilized by Federal agencies considering an investment in Public Key Infrastructure (PKI) on smart cards for governmentwide applications. The Chief Information Officer (CIO) Enterprise Interoperability Emerging IT Committee plans to use the methodology presented herein to help these agencies build business cases that examine using smart cards in concert with the emerging Federal PKI to provide Government employees with a standard identification card to be used for authentication, access control, and electronic commerce (e-commerce). The intended audience of this report is investment decision makers of Federal agencies that are seeking information assurance solutions for their agencies and those practitioners charged with developing business cases.

This report was prepared as a means of helping Federal agencies understand the components for building a sound business case for using PKI/smart cards (cryptographic smart cards) within Federal agencies. By following the business case methodology presented in this document, decision makers will be able to determine for themselves whether the investment costs for PKI/smart cards are justified and whether investment benefits outweigh the risks. Decision makers are also given guidance on evaluating the economic impact of alternatives, comparing alternatives, and ultimately monitoring the investment.

ES.1 BACKGROUND

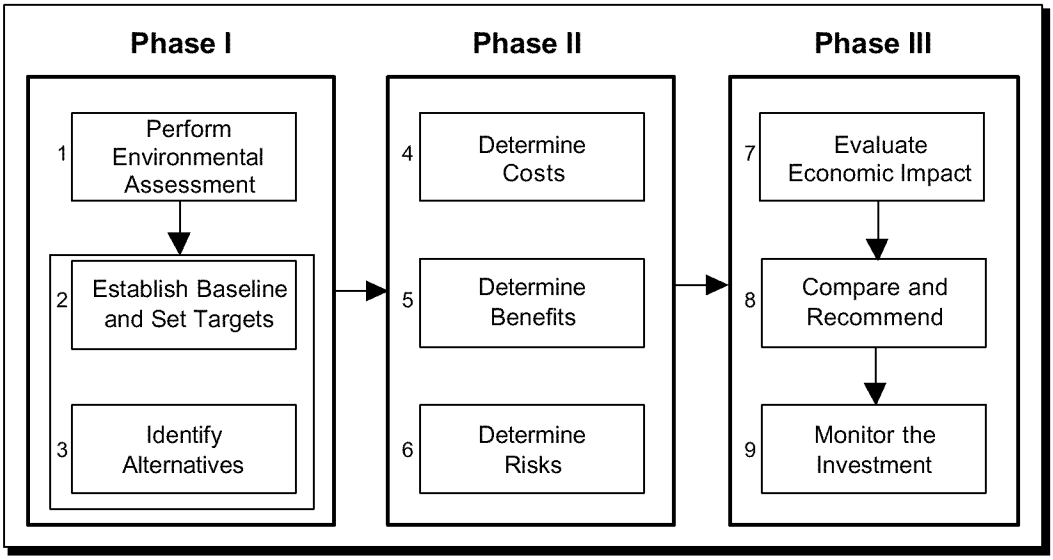
Technological advances and recent legislation like the Government Paperwork Elimination Act have pushed Federal agencies into making e-commerce a reality. Technology and infrastructure are in place to support initiatives such as paperless contracting, wide-area workflow, and the expansion of the governmentwide commercial purchase card program. E-commerce represents a radical change to the way business has been conducted within the Federal Government. To support this radical change, Federal agencies are being required to increase overall network security including providing information assurance. Electronic authentication issues are leading many agencies to consider PKI/smart cards as a probable solution to the security challenges presented by e-commerce. While it is possible to use PKI without smart cards or vice versa, this report focuses on the joint use of PKI and smart cards.

ES.2 METHODOLOGY

A business case analysis is simply an extended form of cost-benefit analysis that considers factors beyond financial metrics. Other factors to be considered might include security needs, business needs, associated risks, and qualitative benefits resulting from the investment. At its core, however, any business case analysis is founded on a comprehensive economic analysis; thus, the business case methodology will examine PKI/smart cards in the context of its investment worthiness as well as its technical and programmatic feasibility.

The step-by-step business case methodology is shown Figure ES-1.

Figure ES-1: Business Case Analysis Methodology for PKI/Smart Cards

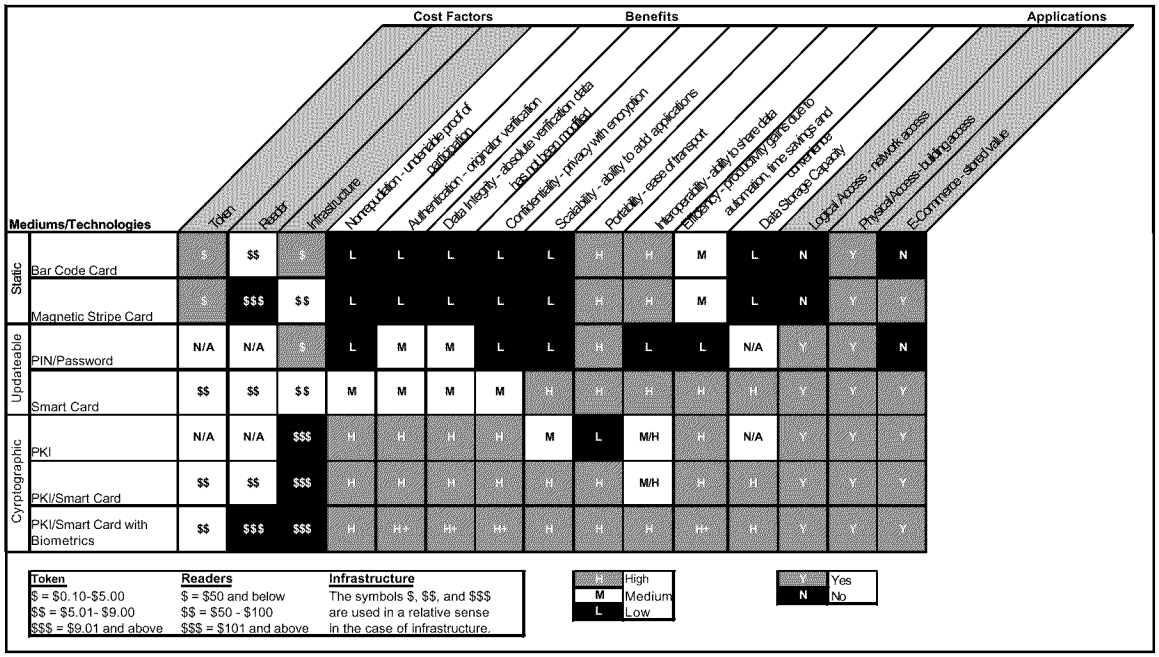


To help create a persuasive business case, this report outlines salient issues related to cost, benefits, and risks. Additionally, this report presents as supporting data two case studies to demonstrate the business case process for PKI/smart cards. Case studies are presented for a large agency and for the Federal Deposit Insurance Corporation (FDIC).

ES. 3 SUPPORTING DATA

To begin, an agency must clearly understand the need for change within its organization and consider the full spectrum of information assurance technology solutions that exist to meet its need. PKI/smart cards are not the only technology that can be used for information assurance. Because there is no one-size-fits-all security solution for Federal agencies, an environmental assessment of the agency should be conducted to determine whether it is a good candidate for implementing PKI/smart cards. Ultimately, the technology selected should best respond to a particular agency's threat environment. PKI/smart cards are useful to agencies that have a mobile workforce with access to card readers (taking advantage of the portability of smart cards), agencies placing a high value on building access, and those that conduct business electronically outside of their agency. The more an agency transacts business with other organizations, the greater the need for strong authentication and nonrepudiation. Furthermore, some agencies have a high need for data integrity and data confidentiality. All of these factors point to the necessity for information assurance solutions that can be addressed through use of PKI. Relevant technology solutions are compared in Figure ES-2 according to the cost of tokens, readers, and infrastructure. Security and operational benefits are also scored for each technology. The technologies are shown in ascending order of information assurance.

Figure ES-2: Viable Alternatives for Information Assurance Solutions



In this figure, three mediums of technology are compared: static (cannot be changed), updateable (can be changed), and cryptographic (can be both changed and programmed). The technologies are listed in order from least secure (bar code cards) to most secure (PKI/smart cards with biometrics). For each technology, the relative cost of a token, reader, and infrastructure is scored. The color schematic uses green for most desirable (lowest costs), yellow for desirable (modest costs), and red for least desirable (highest costs). This matrix shows how cryptographic technologies deliver the most security and operational benefits to agencies, albeit at a higher cost. The full range of alternatives sought should reflect an agency's business need and the requirements of its funding approval body. A more exhaustive discussion of costs is found in Section 4, Cost Analysis.

This matrix also scores the benefits of each technology. First, four security benefits are evaluated according to each technology: nonrepudiation, authentication, data integrity, and confidentiality. These benefits map primarily to PKI. The second section of benefits concerns operational and business benefits realized more through the use of smart cards. These benefits include scalability, portability, interoperability, efficiency, and data storage capacity. Technologies yielding the least benefits were scored red; those with some benefit were scored yellow; and those with the most benefit were scored green. The security and operational benefits are presented for PKI/smart cards in detail in Section 6, Benefits Analysis.

Planning, application enabling, and operational capability are the three most significant costs categories associated with PKI/smart cards. Planning costs include:

- Policy development
- Implementation plans
- Test and acceptance plans
- Bid evaluation strategy, communication, and review
- Award negotiation.

Application enabling costs cover program management, hardware, software, support, and include:

- Program management
- Toolkits
- Application upgrades
- Installation/modifying applications
- Smart cards
- Card readers
- Card issuance workstations
- Test and evaluation
- Support and helpdesk
- Upgrade/product improvement/refresh.

Operational capability costs include:

- Program Management
- Concept Exploration (Pilot)
- Training – System Administrator
- Training – End User
- Documentation
- Auditing
- Helpdesk Support
- System Administration
- Vendor Relations Management.

The cost of fielding PKI/smart cards for an agency with 10,000 employees was estimated to be approximately $1.4 million (in constant dollars) in hardware costs.

Figure ES-3: Illustrative Cost of PKI/Smart Cards

Cost of PKI/Smart Cards (Constant Dollars)					
		Unit Cost	**Quantity**		**Total Cost**
Cost of tokens	$	15	10,000	$	150,000
Cost of network readers	$	75	10,000	$	750,000
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	200,000		$	200,000
Cost of issuing certificates	$	125,000		$	125,000
Total Cost				***$***	***1,425,000***

PKI technology offers the benefits of authentication, nonrepudiation, data integrity, and confidentiality. PKI enables agencies to make full use of the Internet as a means of transacting business in a secure environment. When PKI is implemented with smart cards, additional operational benefits are realized, including scalability, portability, interoperability, efficiency, and data storage capacity.

Beyond considering the costs and benefits of PKI/smart cards, risk should be considered. It is important to consider fully each alternative's risks so that these risks can be properly managed and addressed during implementation. In fact, cost, benefits, and risks associated with each alternative should form the basis of an agency's decision criteria when selecting a preferred alternative. To compare the cost of alternatives, return on investment is often the most effective measure as it provides a means of comparing alternatives with different expenditure streams. Once a preferred alternative is selected, procured, and fielded, the investment should be monitored to ensure that it performs as planned.

In addition to identifying the elements that must be factored into a PKI/smart card business case analysis, Booz·Allen performed two case studies on PKI/smart card use. Case studies are presented for a large agency and for the Federal Deposit Insurance Corporation (FDIC). These case studies are provided to help decision makers and those developing the business case analyses understand the policy implications, technology issues, and the cost, benefit, and risk factors other agencies have already considered in implementing their own PKI/smart card infrastructures. The large agency was selected to represent a large organization that is using PKI/smart cards for logical access and personal identification. Another important factor was the way that the large agency is using smart cards externally as a primary means of delivering benefits to its constituency and providing other benefits like tuition reimbursement.

The large agency is deploying a large PKI/smart card program that services users outside of the agency and expects to spend about $81 million on PKI/smart cards over the next two years. This agency decided to outsource its key management function. Figure ES-4 provides an overview of the their costs for PKI/smart cards for the next two years.

Figure ES-4: Overview of a Large Agency PKI/Smart Card Program Costs

Large Agency - OVERVIEW OF COSTS	Year 1 FY 2001	Year 2 FY 2002
Project Planning	309,101	
Applications	5,067,760	64,016,925
Operational	3,374,443	7,103,365
Certificate Life Cycle	300,000	1,500,000
Total Costs by	***$ 9,051,304***	***$ 72,620,290***

Notes:
1. Received 100,000 certs for FY 2001 from the Customer Advisory Board. Thus Year 1 costs are only transaction fees.
2. In FY 2002 VA will have to issue 134,000
3. One time PKI enabling costs of $200,000 is an approximation.
4. All costs are draft numbers as they are not yet funded and are subject to change.

In contrast to the large agency, the FDIC is a smaller agency with a very mobile workforce—namely, the more than 3,000 bank examiners who travel the country extensively to perform audits at FDIC insured banks. The data resident on a bank examiner's laptop is very sensitive—so much so that the data is worth far more to the agency than the laptop itself. In light of that fact, FDIC uses PKI technology to encrypt this data so that its confidentiality can be ensured should the laptop be stolen or misplaced. Furthermore, FDIC uses PKI/smart cards for logical access, physical access, and personal identification. These two agencies with two business models have addressed their needs through one technology. Although the size of the agencies varies greatly, it demonstrates one of the major benefits of PKI/smart cards: scalability.

For both case studies, the cost of developing a certificate policy, establishing a PKI, and distributing smart cards is presented. The relative benefits the agencies perceive they derive from the new technology are discussed. The case studies describe two distinct approaches. The large agency has pursued outsourcing of key management whereas FDIC has decided to manage its own program. FDIC employed the technology during its infancy stage and will take a little more than four years to stand up PKI/smart card infrastructure fully—estimated date is March 2001. On the other hand, the large agency

did not begin to build its PKI/smart card infrastructure until June 2000, but the agency is on an accelerated plan to be fully operational in only 18 months. The path an agency takes may be different from these, depending on security requirements, user population, and business needs.

FDIC expects to spend almost $7.5 million on PKI/smart card technology over the next two years. Figure ES-5 below shows a breakdown of FDIC's expenditures on PKI/smart cards for the next two years.

Figure ES-5: Overview of FDIC PKI/Smart Card Program Costs

FDIC: OVERVIEW OF COSTS		
	Year 1	**Year 2**
	FY 2000	**FY 2001**
Project Review		
Planning		
Applications Enabling	1,457,000	1,678,300
Operational Capability	3,550,000	800,000
Certificate Life-Cycle Management		
Total Costs by Year	***$ 5,007,000***	***$ 2,478,300***

Notes:

1. Planning and project review costs were not direcly assigned to PKI smart cards project.
2. Certificate life-cycle management is part of Vendor relations management costs.
3. Year 1 costs include the cost of the ETV pilot of $2.75 million.

These case studies show that implementation of PKI/smart card technologies is achievable, beneficial, and affordable. FDIC and the large agency demonstrate that PKI/smart card technology is achievable in a relatively short fielding time. The technology has improved operations, streamlined business processes, and even reduced costs. At FDIC the cost savings from the use of PKI and digital signature for electronic travel vouchers almost paid for the entire PKI infrastructure. Finally, PKI/smart card technology is affordable. The total costs of PKI/smart card technology cost each agency on average approximately $425 per user each year. As an agency builds its own business case for PKI/smart card technology, the case study information provided and the lessons learned shown in this paper should be drawn upon.

1. INTRODUCTION

1.1 PURPOSE

This report was prepared as a means of helping Federal agencies understand the components for building a sound business case for using PKI/smart cards (cryptographic smart cards) within Federal agencies. This report provides decision makers with a framework to construct a business case and provides detailed information on the costs, benefits, and risks associated with both PKI and smart card technologies. By following the business case methodology presented in this document, decision makers will be able to determine for themselves whether the investment costs are justified and whether the benefits outweigh the risks. Decision makers are also given guidance on evaluating the economic impact of alternatives, comparing alternatives, and ultimately monitoring the investment.

1.2 SCOPE

This report focuses on the joint use of PKI and smart cards. It is possible to use PKI without smart cards or vice versa, but this report strives to show how the two can be used synergistically to benefit agencies. This report provides an approach for determining the costs, benefits, and risks of PKI/smart cards. This report does not actually show a business case analysis; it explains how to conduct one. A brief discussion of alternative technologies is also provided. Two case study examples are provided of Federal agencies that are implementing PKI/smart cards.

1.3 DOCUMENT LAYOUT

The *Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications* comprises nine main sections.

- **Section 1—Introduction:** Presents the purpose and scope of the document.
- **Section 2—Business Case Analysis Methodology:** Describes the methodology an agency can use to make an investment decision regarding PKI/smart cards. The steps in the methodology are performing an environmental assessment; establishing a baseline; identifying alternatives; determining costs, benefits, and risks; evaluating economic impact; comparing alternatives and formulating recommendations; and finally, monitoring the investment.
- **Section 3—Environmental Assessment, Baseline, and Alternatives:** Discusses the legislative changes, market changes, and other factors that have spurred the implementation of PKI/smart card solutions. A range of alternatives is presented so that the benefits of using PKI/smart cards can be better understood.
- **Section 4—Cost Analysis:** Provides a sample cost element structure for PKI/smart cards and shows the relative equipment costs of magnetic stripe cards, smart cards, PKI/smart cards, and PKI/smart cards and biometrics.

- **Section 5—Benefit Analysis:** Describes the security benefits associated with PKI and the operational benefits associated with smart cards.
- **Section 6—Risk Analysis:** Explains the risks stemming from use of smart card and PKI technologies.
- **Section 7—Impact of Investment:** Shows how a final investment decision is made by comparing the cost, benefits, and risks of alternatives and the baseline.
- **Section 8—Case Studies:** Relates how a large agency and FDIC have implemented PKI/smart card technology within their agencies. An implementation timeline, costs, benefits, and risks are shown.
- **Section 9—Conclusion:** Summarizes the findings in the document.

Every section of this report ties back to the business case methodology presented in Section 2. This report was designed in this fashion to help agency personnel build a sound business case.

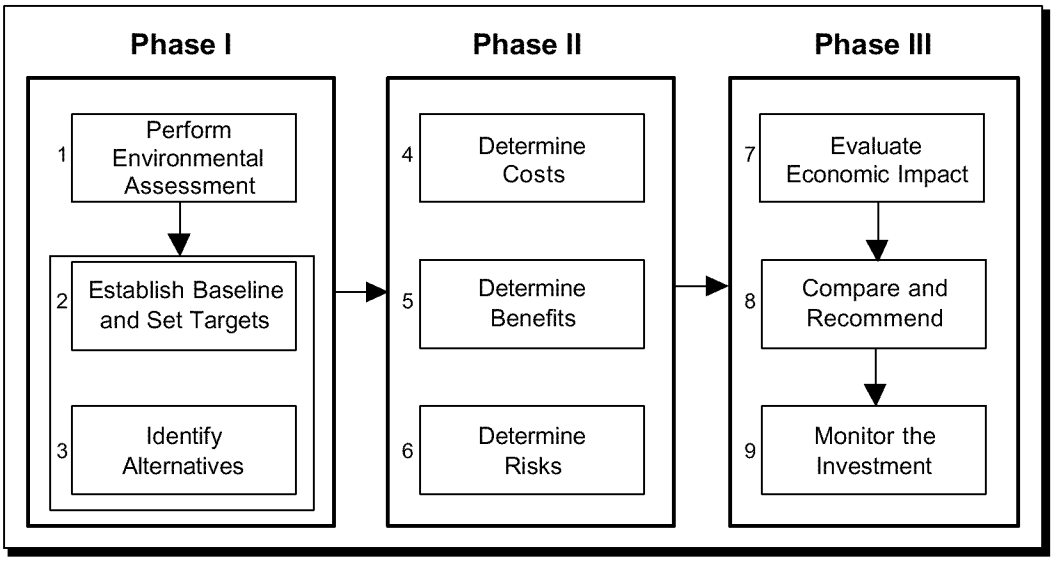
2. BUSINESS CASE METHODOLOGY

Business case analyses often help to answer the following questions:

- Are there environmental factors that influencing the investment decision, such as legislation or regulation?
- What technical, business, and regulatory factors are germane to the technology being investigated (i.e., PKI/smart cards)?
- What feasible alternatives can meet the business and process needs of your agency?
- What are the relevant costs associated with each alternative?
- What is the realistic life of the technology (e.g., PKI/smart card project) and can costs and benefits accurately be predicted over this time period?
- What are the cost risks associated with the estimates?
- What are the relevant benefits associated with each alternative [e.g., enhanced security, productivity improvements, uniformity of process, and future applications (e.g., PK-enabled applications)] and have all those associated benefits been quantified/assessed?

The three-phased business case methodology shown in Figure 2-1 represents a composite of the best practices found in government and industry which are applicable to PKI/smart card technology. As agencies build their own business cases for PKI/smart card programs, the steps identified below will help document the business rationale for these investments.

Figure 2-1: Business Case Analysis Methodology for PKI/Smart Cards



This PKI/smart card business case methodology is simply an extended form of cost-benefit analysis that considers factors beyond financial metrics. Other factors to be considered might include security needs, business need, associated risks, and qualitative benefits resulting from the investment. At its core, however, any business case analysis is founded on a comprehensive economic analysis; thus, the technical approach presented in the following paragraphs is organized according to each of the steps in the business case analysis.

Step One: Analyze the Current Environment and Assess Affected Areas

The first step is to conduct an analysis of the current environment and an assessment of affected areas. It is critical to understand the current business processes and technologies in place and to determine the shortfalls or deficiencies associated with the current environment. Environmental assessments can include reviewing technology inventories, architectures, business processes, etc. Almost every investment, either in facilities, personnel, technology, or knowledge affects numerous parts of the organization. Organizational implications (costs and benefits) must be assessed. Understanding how a potential organizational change impacts the current environment is critical to evaluating the return on investment and the expected short and long-term values of the project.

Data needed for this and all other steps of the business case analysis can be collected through a number of mechanisms including:

- Financial analysis of program data
- Documentation review
- Survey responses from the stakeholders
- Market research
- Interviews.

Step Two: Establish a Baseline and Set Targets for Improvement

To obtain the relevant costs and associated benefits of implementing PKI/smart card within an agency, a baseline for comparison must be established. This can be done by comparing the findings concerning the current environment with stated objectives for an agency or program. The outcome of the comparison enables shortfalls of the current environment to be determined and opportunities for change to be identified. By doing this, an agency demonstrates why it needs PKI/smart cards rather than other technologies. The discussion should point to business drivers, security drivers, and technology drivers that led to the conclusion to pursue this solution. For example, the use and applicability of PKI/smart cards across the Federal Government for physical access, logical access, and digital signatures as it relates to an agency's business needs should be addressed. This information is often collected by interviewing business process owners and functional proponents of the business units potentially affected by

the use of PKI/smart cards. Investment objectives should be stated to define the goal of the investment and how it is an improvement over baseline operations.

Step Three: Identify Viable Alternatives

In this step, all options to achieve an agency's stated information assurance goals should be captured. At this stage, many alternatives can be considered, from the low-end technology solutions (e.g., bar codes) to the high-end smart cards with biometrics to multiple combinations in between. Cost and feasibility should not preclude an alternative from consideration.

Once all potential alternatives have been identified the agency must follow a process to narrow the realm of possibilities down to a few viable alternatives. Using the data collected previously, alternatives can be evaluated on their ability to fill the gaps between where an agency is now and where it wants to be in the future. Asking whether the organization can absorb the change and gauging the probable long-term success of the investment are critical actions before starting to calculate costs and benefits. Other factors used to determine viability include technical or programmatic feasibility, cost, regulatory compliance, etc. This first analysis can reduce the range of alternatives to a manageable number that can then be more fully quantified. The remaining alternatives always include baseline operations (e.g., status quo alternative) in addition to at least one potential investment alternative.

Step Four: Determine the Costs

The costs of continuing the current process (status quo) and each of the viable alternatives need to be calculated for a determined period of time (e.g., 10 year life cycle). To do this, a cost element structure needs to be created as a framework for equitable comparisons. This structure should be designed specifically for PKI/smart card initiatives. Section 4, Cost Analysis, provides an illustration of costs associated with PKI/smart cards. When the cost element structure is in place, you need to collect appropriate cost data for each alternative. A cost model should be built to calculate costs. Sometimes, verifiable cost data are not available, and costs need to be derived by proxy or estimation. It is a good business practice to mitigate cost risk so your cost estimate is not skewed as a result of poor assumptions.

Step Five: Determine the Benefits

Benefits and cost savings/avoidance need to be identified for continuing current operations (the status quo alternative) and for each of the viable alternatives. The business case assumes varying levels of benefits for each alternative in addition to varying costs. To the fullest extent possible, an agency must identify and quantify benefits that will be derived from alternative investments made in implementing PKI/smart cards. Section 5, Benefit Analysis, provides an explanation of some probable benefits. Keep in mind that many benefits realized through a particular alternative will be qualitative and will not lead directly to dollar savings. Improvements in customer service, regulatory compliance, security, and accountability are certainly recognized as

benefits, but they rarely can be included in the dollar-valued benefits stream or return on investment (ROI) measures. These qualitative benefits can be numerically scored by assigning a value to fully meeting, partially meeting, or not meeting stated business or functional drivers. These benefits should be highlighted in the final report and should be considered in selecting the preferred alternative.

Step Six: Determine the Risk

The purpose of a risk analysis is to focus the decision maker's attention on the financial, technical, and schedule risks associated with the alternative under study and to counter-balance positive financial indicators with real-world factors that could keep the alternative from reaching its estimated potential. Taking a proactive management approach to risk is consistent with industry best practices of instituting a risk management process and employing best-of-class risk management methodologies to ensure that appropriate risk mitigation strategies are implemented and project goals are achieved.

Because any look into the future involves an inherent level of uncertainty, business case analyses are subject to risk. Identify the risks associated with the PKI/smart card investment so that they can be managed and controlled. Use cost risk analysis tools to account for any cost risk associated with your estimates.

Step Seven: Evaluate the Economic Impact of the Investment

When all of the cost components have been identified, the status quo should be compared with the viable alternatives. The most useful financial results in a business case appear in a time-based cash flow summary.

Economic impact indicators can be used by decision makers to evaluate an investment based on absolute dollar impact and dollars over time, as well as how quickly the investment dollars are recovered. Examples of economic impact indicators include cost savings, cost avoidance, return on investment, payback period and cost benefit ratios.

It is important to remember that the specific financial measures used to evaluate the investment are simple calculations based on complicated assumptions. For example, in estimating the costs, are desktop system upgrades that were needed for other purposes included? Or the implementation of a new directory service that has value for applications other than PKI? It is often very difficult to isolate the costs of PKI per se. Given this, every effort should be made to ensure that estimates fully state the assumptions on which they are based.

Step Eight: Compare and Recommend an Alternative

After the economic impact of each alternative has been established, the alternatives can be compared with one another as well as with the status quo, and an investment recommendation can be presented. The comparison of alternatives is completed by calculating the net present value for each, comparing the ROI, and identifying which alternative benefits the organization the most. This comparison should include a

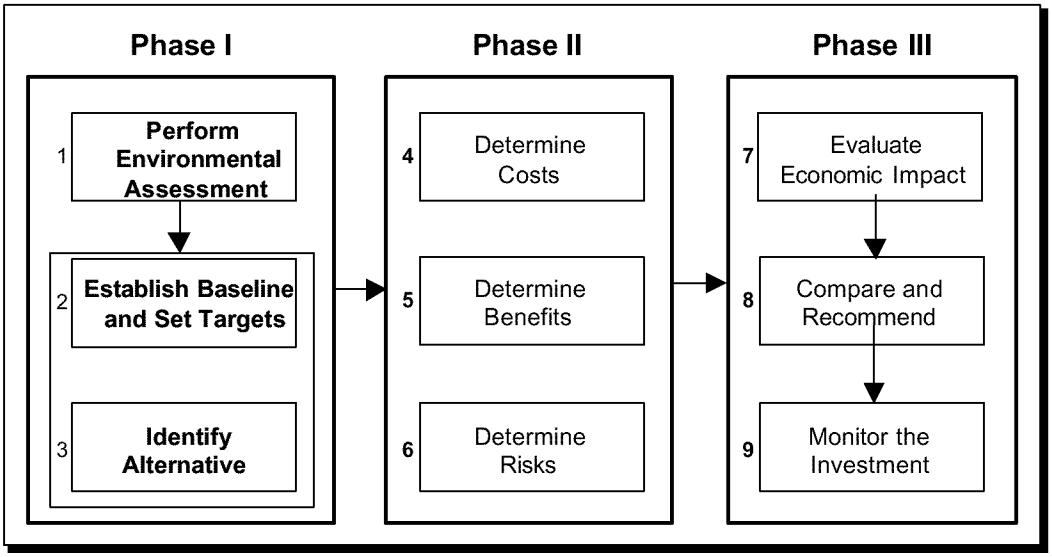
thorough look at the intangible benefits and increases in effectiveness that cannot be assigned a dollar value. The preferred alternative can then be used to support the budgeting process as dictated by Office of Management and Budget (OMB) Circular A-11 and can provide the basis for managing results as stated in the Government Performance and Results Act.

Step Nine: Monitor the Investment

When the preferred alternative has been selected, approved, funded, and fielded, the agency's job is not over. The investment should be monitored to ensure that it is achieving stated cost and performance goals (e.g., that the investment continues to provide value to your organization.) Some agencies set up performance measures or information assurance security metrics that provide on-going assessments of the value and performance of the investment. Often, failure to monitor the investment carefully leads to less than expected returns. Therefore, it is extremely important to review the investment's performance over the life of the project.

3. ENVIRONMENTAL ASSESSMENT, BASELINE, AND ALTERNATIVES

Figure 3-1: Phase I Business Case Analysis Methodology for PKI/Smart Cards



3.1 ENVIRONMENTAL ASSESSMENT

During Phase I of a business case, an environmental assessment should be performed by mapping representative current processes to the operating environment. These maps will be used to demonstrate how PKI/smart cards are needed for your agency vice other technologies. The discussion should point to business drivers, security drivers, and technology drivers that led to the decision to pursue PKI/smart cards. For example, a case for change may be based on:

- Need to improve security posture within your agency
- Requirement to comply with legislative, executive, and agency guidance
- Ability to accomplish mission
- Participation in e-government initiatives.

Some agencies conduct security audits and/or vulnerability assessments to assess their present security posture. This provides the impetus for change that decision makers often require and should be described in great detail in the business case.

Security breaches are very damaging to an agency's reputation as they receive signficant media attention. For example, in October 1999, U.S. officials revealed that hackers had systematically penetrated the security mechanisms of the Department of Defense (DoD) computers for more than a year and had downloaded vast amounts of proprietary information. The National Aeronautics and Space Administration (NASA) and the Department of Energy were affected as well as the Pentagon. According to the

Washington Post, an FBI-led inquiry code named "Moonlight Maze" has not been able to identify the cyber-attackers or whether espionage was the motive. Although no classified data is known to have been stolen (some of the files apparently downloaded include bidding documents and contracts), this incident highlights the need for greater information assurance capabilities within the Federal Government.

In response to this incident, the DoD ordered $200 million in new encryption technology, and upgraded intrusion-detection devices and computer firewalls to prevent unauthorized use of its networks. It is believed that the widespread use of the Internet has created enormous new opportunities, as well as frightening vulnerabilities, for agencies around the world. While firewalls protect infrastructure and communication lines, encryption capabilities like PKI protect the actual transmission of data.

A primary reason why information security has become elevated in importance to agencies is that e-commerce has grown exponentially over the past few years, with business-to-business e-commerce reaching $43 billion and business-to-consumer e-commerce reaching $8 billion in 1998. It is predicted that these totals will exceed $108 billion and $1.3 trillion respectively by 2003 (Forrester Research). As a result, Government agencies must implement technology that will electronically enable their services in a secure fashion.

3.1.1 Improve Security Posture

Agencies must improve their security posture by ensuring the integrity and confidentiality of their data, validating all users who wish to access data, and by providing a means for digital signatures that cannot be repudiated at a later date. For example, digital signature provides an audit trail which allows one to determine which user performed a specific action, and under whose authority that action was performed. The security improvements realized through the use of digital signature provide agencies and their stakeholders greater confidence in the integrity of their systems and the accuracy of their data. Further, agencies will be confident that their data is being used as intended. Without these improvements in security posture, agencies will not be able to become a true competitor in the new e-commerce economy by participating in e-government initiatives.

3.1.2 Comply with Legislation, Executive, and Agency Guidance

The use of PKI/smart cards is being prompted by recently enacted legislative, executive, and agency policies. For example, PKI certificates can be used to comply with the Government Paperwork Elimination Act (GPEA, Public Law 105-277). This act requires Federal agencies to accept electronic signatures, including digital signatures. Further, GPEA asserted that electronic signatures would not be denied legal validity simply because they are in electronic form (and this point was reinforced through the enactment of the Electronic Signatures in Global and National Commerce Act in June 2000, covering transactions between private parties, such as businesses and consumers). GPEA required agencies to submit plans to OMB by October 2000 as to how they would comply with the act. Using PKI is one way agencies can comply with

GPEA. Subsequent presidential administration directives reinforced the need for acceptance of electronic forms with electronic signatures. OMB has issued guidance (Federal Register May 2000: Volume 65, Number 85, page 25508) for the use of electronic signatures to facilitate adoption by Federal agencies.

Digital certificates provide a means for authenticating transacting parties over the Internet, and thus conducting business with confidence over the Internet. Public key technology enables digital signature functionality that provides authentication of electronic data for a wide variety of applications. The use of digital signature without public key technology may compromise authentication and lack nonrepudiation capability. Further, a single infrastructure provided by PKI supports both digital signatures and confidentiality (preferably using two different key pairs and certificates). As a result, many agencies are inclined to use public key technology as a solution. Although the deadline for compliance with the mandates of GPEA is three years away, the passing of the act and the OMB requirement for an implementation plan have encouraged Federal agencies to consider seriously digital signatures.

Furthermore, agencies must also comply with the provisions of Presidential Decision Directive (PDD) 63, which mandates that critical infrastructures of the United States must be protected against terrorist attack. Certain information systems are identified as a critical infrastructure, as is the continuity of government operations. Information assurance is often a key component of an agency's critical infrastructure plan. The encryption of data via PKI/smart cards is one way agencies can comply with PDD-63 requirements to protect critical infrastructure against terrorist attack.

Some agencies are also issuing guidance that is driving promulgation of PKI/smart cards. In the DoD, for example, a memo from Dr. John Hamre requires that PKI-enabled via a common access card be issued to all active duty military, reservists, and civilians and contractors employed at the DoD by the end of 2002.

3.1.3 Accomplish Mission

Improving your agency's security posture is consistent with the mission of the Federal Government. Providing high-quality customer service is a top priority for many agencies. Agencies can vastly improve the level of customer service they provide by:

- Providing a means for completing forms over the Internet
- Ensuring the integrity of the data provided to customers
- Guaranteeing that confidential data will not be compromised
- Validating that users attempting to gain access to systems are authorized users.

Many agencies responsible for national security, including the DoD, can accomplish their mission more effectively by implementing technologies that will greatly enhance their security posture. For example, it is imperative for agencies with national security missions to guarantee the confidentiality of classified data, protect engineering secrets, and prohibit unauthorized users from gaining access to data. However, all agencies

can meet mission objectives more effectively by providing a means to complete transactions securely over the Internet, ensuring the integrity and confidentiality of the data, and properly authenticating all users.

3.1.4 Participate in E-Government Initiatives

As Federal agencies use the Internet to transact business, effective user authentication, confidentiality, data integrity, and nonrepudiation become critical security objectives. The widespread use of the Internet necessitates information assurance improvements, These include the ability to verify that communicating parties are who they claim to be and the ability to accept forms that have been digitally signed and will be legally binding. Further, organizations must be able to ensure the confidentiality of business transacted over the Internet and to protect this data from tampering. PKI facilitates e-commerce in that it can provide security services for electronic communications and the electronic exchange of information between parties, including those who do not have a previously established relationship. Public key technology helps organizations to accomplish all of these things, thereby becoming a catalyst for the e-government marketplace.

3.2 ESTABLISH BASELINE AND SET TARGETS

Interviews should be conducted throughout your agency and baseline processes mapped. In addition to determining existing business processes, baseline costs associated with the business process should also be collected. Baseline costs will be the basis against which ROI will be determined.

Before embarking on any investment path, performance targets should be set. These targets may be expressed in the form of goals. Any number of goals might be developed, and the potential opportunities derived from the use of PKI/smart cards can be grouped into categories, such as:

- Information integrity, security, tracking, and accountability
- Authorization and access control
- Process improvement and standardization
- Customer service and quality
- Cycle and processing time.

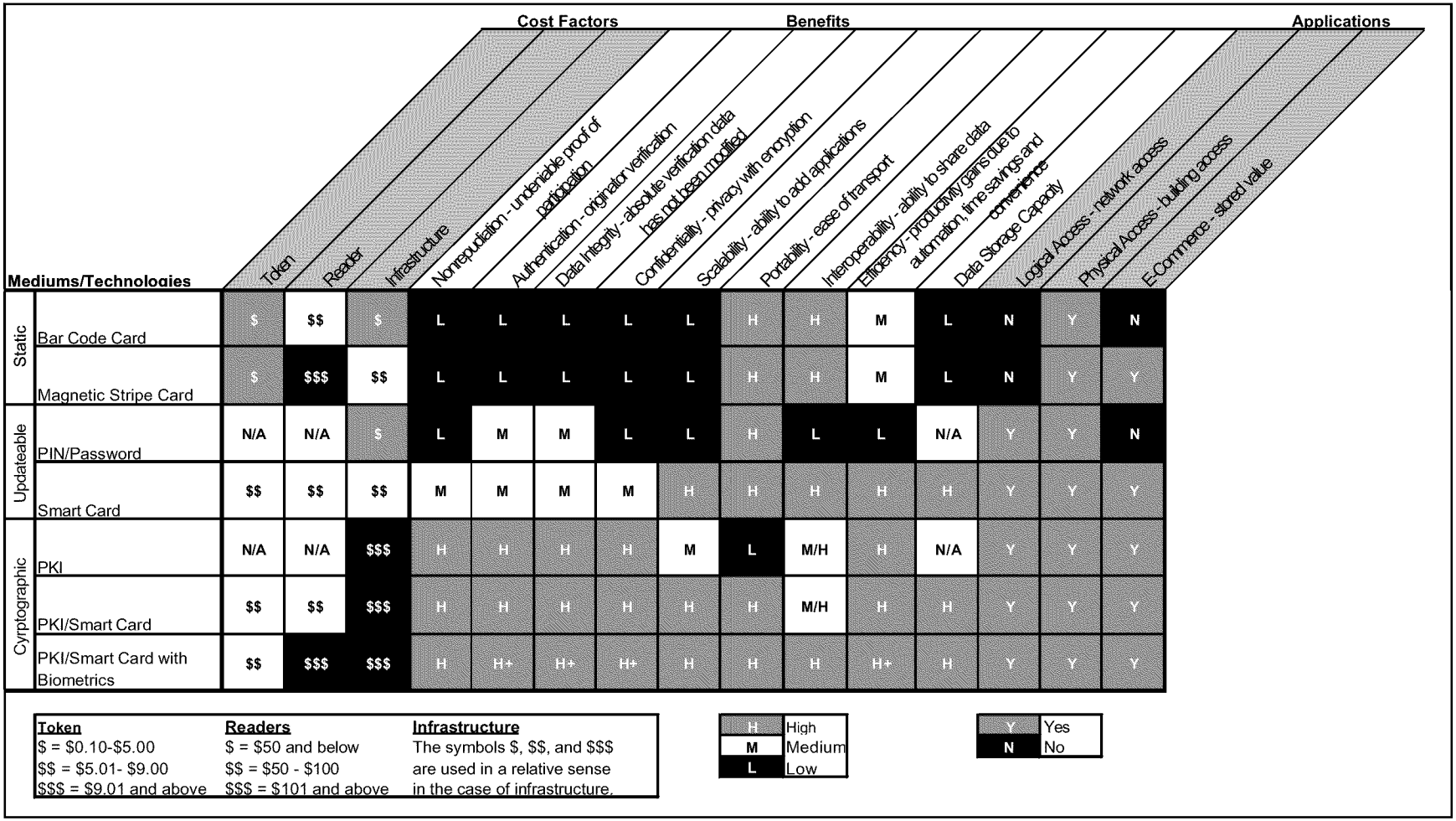
When the opportunities for change have been identified, potential solutions to implementing PKI/smart cards for governmentwide applications should be developed. These solutions eventually become the investment alternatives and typically arise from extensive group brainstorming sessions and interviews.

3.3 INFORMATION ASSURANCE ALTERNATIVES

Although this report focuses on PKI/smart cards, it is possible to achieve aspects of authentication, data integrity, confidentiality, and nonrepudiation using other technologies. Other security protection alternatives include bar code cards, magnetic stripe cards, PIN/password, non-PKI-enabled smart cards, and biometrics. Although all of these alternatives provide some means of information assurance, only PKI provides a high degree of assurance in all areas. When technologies are layered by using the technologies in combination (e.g., PKI, PIN/password, and biometrics), a greater degree of assurance can result. Figure 3-2 shows the relative costs, benefits, and potential applications of each (potential) alternative.[1] The technologies introduced in Figure 3-2 to help agencies build a broad range of information assurance alternatives into their business case.

1 Source: Booz·Allen & Hamilton

Figure 3-2: Viable Alternatives for Information Assurance Solutions



In Figure 3-2, three mediums of technology are compared: static (cannot be changed), updateable (can be changed), and cryptographic (can be both changed and programmed). The technologies are listed in order from least secure (bar code cards) to most secure (PKI/smart cards with biometrics). For each technology, the relative cost of a token, reader, and infrastructure is scored. The color schematic uses green for most desirable (lowest costs), yellow for desirable (modest costs), and red for least desirable (highest costs). A more exhaustive discussion of costs is found in Section 4, Cost Analysis.

In addition to cost, Figure 3-2 scores the benefits of each technology. First, four security benefits are evaluated according to each technology: nonrepudiation, authentication, data integrity, and confidentiality. These benefits map primarily to PKI. The second section of benefits concerns operational and business benefits realized more through the use of smart cards. These benefits include scalability, portability, interoperability, efficiency, and data storage capacity. Technologies yielding the least benefits were scored red; those with some benefit were scored yellow; and those with the most benefit were scored green. The security and operational benefits are presented for PKI/smart cards in detail in Section 6, Benefits Analysis.

The columns entitled “Applications” at the top right of Figure 3-2 show the potential uses of the technology for logical access to networks, physical access to buildings, and electronic commerce. 'N' denotes limited, if any, application and 'Y' denotes extensive application.

3.3.1 Bar Code Card

A bar code card is a standard credit-card-sized device with a printed code used for recognition by a bar code scanner. The scanner reads bar codes and converts them into either the ASCII or EBCDIC digital character code. Bar code cards are used for applications that require personal or product information. Although bar code tokens are inexpensive and highly portable, they do not offer security benefits (e.g., authentication, and data integrity).

3.3.2 Magnetic Stripe Card

A magnetic stripe card is a standard credit-card-sized device that adheres to standards approved by the International Standards Organization (ISO) to encode digital data on a magnetic strip that is embedded on the card. Data is written on and read from the stripe by a number of types of readers at the time of transaction. Currently, magnetic stripe cards are used for applications such as banking, retail, telephone systems, access control, airline ticketing, and transit fare collection. The life span of a card will vary depending on its intended use. For example, a card may be intended for one-time use (e.g., a subway pass) or for thousands of transactions; however, the typical magnetic stripe card must be replaced in less than two years.

3.3.3 PIN or Password

PIN and password technologies are commonly used for numerous Internet and intranet applications due to the fact that these technologies are relatively inexpensive and easy to implement. However, PIN and password technologies are considered to offer only a weak form of authentication. Most users select passwords that are common words and thus susceptible to dictionary attacks. If the PIN or password is either meaningless or really long, it will be harder for the user to remember. As a result, users will write it down or store it on their computer making it easier for imposters to obtain. Users also tend to use the same PIN or password for different applications. Therefore, if an imposter obtains a user's PIN or password, the imposter can gain unauthorized access to multiple applications. Good PIN and password policy can mitigate some of these problems, but enforcement is still difficult at the user level. Passwords phrases are becoming more commonly used as they are easier to remember but more difficult to decipher. Additionally, policies can mandate frequent updates to PINs or passwords.

3.3.4 PKI

PKI is the use of public key cryptography, which employs an algorithmic function to create two mathematically related or complementary “keys.” Federal agencies can use public key technology to deliver functionality such as authentication, data integrity, confidentiality, and nonrepudiation. Public key technology uses a public key and a private key to mathematically scramble data. The private key cannot be determined from the public key. One key is used to encrypt the data, while the other key is used to decrypt it. The key itself is actually a series of numbers/bit strings. One key is public and made available to a trading partner, and the other is kept private and is maintained only by the user.

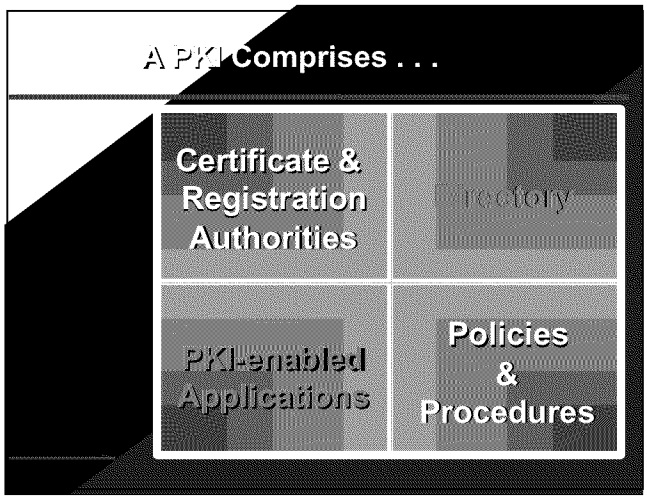
As an infrastructure, PKI comprises Certificate Authorities (CA), Registration Authorities (RA), PKI-enabled applications, policies and procedures, certificate management services, and directories that provide security features such as message integrity, key recovery, data privacy, signature verification, and user authentication (see Figure 3-3.). Each public key is made public in the form of a digital certificate where a trusted party, a CA, cryptographically binds the public key to one’s identity by digitally signing the certificate, thus ensuring any attempts to alter the data will be detected.

A CA manages the following:

- Certificate life cycle (which involves issuing the keys)
- Key revocation when a private key may have been lost, stolen, or made public
- Notice as to which key pairs have been revoked.

Registration authorities register subscribers into a particular CA’s domain. Directories are established that contain the public encryption keys and certificates that are used in verifying digital certificates, credentials, and encryption.

Figure 3-3: Components of PKI

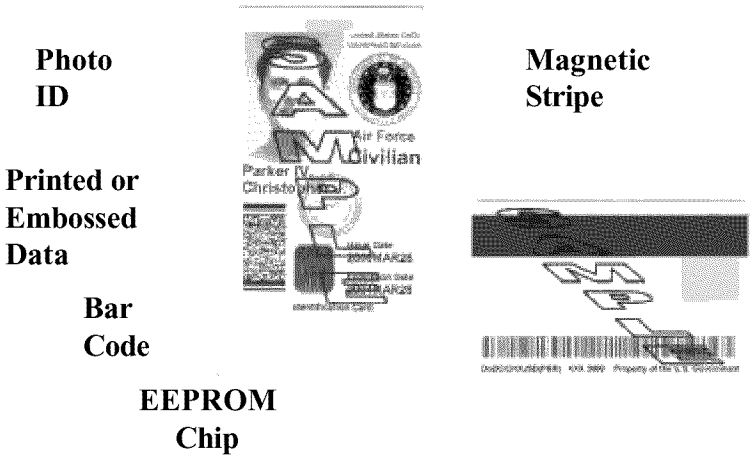


PKI supports digital signature functionality that provides integrity of electronic data for a wide variety of applications. A "digital signature" is derived from the data in combination with the private key and is normally appended to the data that is digitally signed. To verify the signature, the signer's public key is applied to the digital signature. The signing operation is a two-step process: First, the signer hashes the data to a fixed size value. The signer then subjects this value to a private-key operation. Verification is also a two-step process: The verifier hashes the data to the fixed size value. The verifier then examines the value, the transmitted signature, and the signer's public key. If the signature matches the hash value and key, the signature is "verified." Digital signatures provide both proof of authenticity and verification of data integrity.

3.3.5 Smart Cards

Smart cards are credit-card-sized devices that carry an embedded microprocessor and memory that can store and process information. When inserted into a card reader, the smart card transfers data to and from applications. It is more secure than a magnetic stripe card and can be programmed to cease functioning if an incorrect password is entered more times than the preset limit. Smart cards have a wide range of applications including electronic purse, logical and physical access control, health care, telecommunications, and transportation. To date, approximately 700,000 smart cards have been issued within the Federal Government. Figure 3-4 illustrates a typical smart card and its components.

Figure 3-4: Typical Smart Card



Smart cards can be integrated in both physical and logical access control systems. A physical access control system is an automated system that controls an individual's ability to access a physical location, such as a building, parking lot, office, or other designated physical space. A logical access control system is an automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database. Smart cards may use three levels of logical access control:

- The association of a set of privileges with a user's password, and the ability to control access to files on the card based on those privileges (also called file access security)
- The ability to detect and respond to a sequence of invalid access attempts with a self-locking mechanism
- The "logical channel"—a logical link between the host system and a file on the smart card.

The use of smart cards for logical access augments the traditional PIN/password logon process, which was described by Microsoft Chairman and Chief Software Architect Bill Gates in the following manner: "Passwords are the weak link in Internet security. The use of smart cards will become the major way for corporate users to authenticate themselves to the network." (May 9, 2000.)

PKI/smart cards offer an enhanced level of security that includes authentication, confidentiality, data integrity, and nonrepudiation. Files may be readable but not writable or vice versa and only accessible within the card. Files may be protected by one or several passwords (PIN) or biometrics.

Also, PKI/smart cards offer an enhanced level of security because public/private keys can be generated, stored, and used to make digital signatures or encrypt data all on the card. This provides a much higher level of security than non-PKI enabled smart cards

that store keys on a floppy disk or hard drive and are, therefore, more susceptible to tampering, removal, or duplication. Additionally, the portability of the public/private key pair and digital certificates enables users to take advantage of the benefits of PKI at any location where they are an authorized user.

3.4 APPROPRIATE AGENCY TO IMPLEMENT PKI-ENABLED SMART CARDS

A profile of characteristics that would indicate if a particular agency is a good candidate for PKI/smart cards is presented below. If an agency possesses these characteristics, in part or in whole, it should investigate how this technology could benefit the agency as well as consider the applications that could be enabled by the smart cards. Agencies that deal with sensitive data and therefore have a great need for a high level of security are prime candidates for cryptographic smart cards. Examples include agencies that ensure national security, deal with large amounts of money, or maintain substantial databases holding private information on the public.

- **Data Integrity.** If an agency's performance relies on the accuracy of its data, PKI/smart cards should be considered because they enhance the data integrity. Data integrity relates to the reliability of data and ensures that data has not been tampered with. An agency depending on reliable data would benefit from using PKI/smart cards.
- **Confidentiality.** An agency that maintains confidential data (including financial and medical data) is a good candidate for implementing PKI/smart cards. The large agency in the case study is an example of an agency where maintaining confidential data is crucial to delivering high-quality customer service to its millions of beneficiaries.
- **Authentication.** Most agencies have a significant need for authentication or the verification of the identity of a user who is logging onto a computer system.
- **Internet-Based Transactions.** The amount of business transacted over the Internet also is a factor for agencies considering the use of PKI/smart cards. The use of electronic signatures is surging. The *Electronic Signatures in Global and National Commerce Act* gives electronic signatures the same legal weight as hand-written signatures and recognizes e-commerce as a legally binding transaction. As electronic signatures are used to submit forms over the Internet, the need for a higher level of security is greatly increased.
- **Need for Interfacing with Other Federal Agencies.** An agency that has a high level of interaction with other Federal agencies should explore the use of PKI/smart cards. These are agencies that interface with many other agencies and in doing so, exchange large amounts of data. The Federal Bridge Certification Authority (FBCA) provides a means for connecting diverse PKI.
- **Mobile Workforce.** An agency with a significant part of its workforce at multiple locations would benefit substantially from the use of PKI/smart cards. Possible functionality that would benefit this user group includes logical access and physical

access. Additional benefits are gained by the PKI-enabled encryption of data on laptops, making them inaccessible to unauthorized personnel.

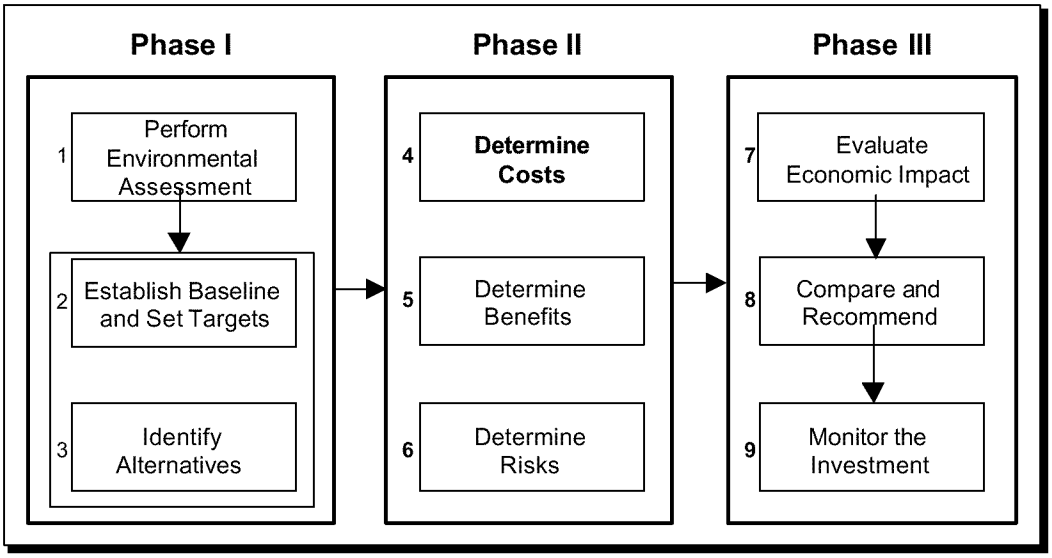
3.5 OTHER CONSIDERATIONS

When an agency has decided to implement PKI/smart cards, it must seek answers to the following questions:

- What functionality should be included?
- How will the keys be managed?
- How will the infrastructure be structured and maintained?
- How will the cards be maintained?

4. COST ANALYSIS

**Figure 4-1: Phase II Determine Costs-
Business Case Analysis Methodology for PKI/Smart Cards**



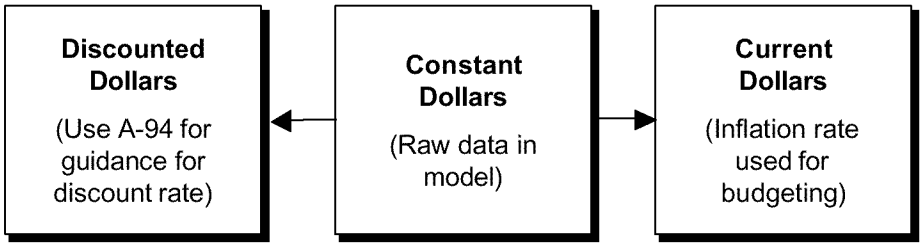
A business case is incomplete without a well-documented section on costs. Most investment decisions rely on the cost analysis as a significant factor in the final decision. Therefore, a life cycle cost estimate should be calculated for each alternative. This total cost should be expressed in constant dollars—meaning *uninflated* dollars—and used to measure the value of purchased goods and services in terms of the price level in a given base year. This is the most appropriate way to evaluate dollars from year to year because the value of the dollar changes over time. Constant year dollars are typically used in economic analyses for estimating purposes and are measured in terms of stable purchasing power on a specific base year. By comparison, current dollars are the cost shown in the dollar value of goods and services in terms of the prices and estimated inflation at the time of purchase.

Current dollars are often used by Federal agencies for budgeting purposes. This view takes into account the effects of inflation and the price levels expected to prevail during the year at issue. Current dollars are used when fiscal year amounts include all increases needed to cover inflation and those price increases expected to occur in a program over the duration of the program at the appropriate outlay rate. The term current dollars may also be referred to as *budget dollars*, *fully inflated dollar*s, and *then-year dollars*.

Discounted dollars (also called present value dollars) are used to compare the costs of different alternatives or to compare costs from different years. Discounted dollars take into account the time value of money that reflects the fact that money in hand today is more valuable than an identical amount of money received in the future. Present value costs are calculated by applying a discount factor to constant year dollars. The discount factor (real rate) translates the expected benefits or costs of the future years into terms

of today's dollars. OMB Circular A-94 provides guidance on the use of discount rates. The relationship between these three views is shown in Figure 4-2.

Figure 4-2: Views for Expressing Total Cost



To compare alternatives equitably, agencies should use a net present value (NPV) calculation of the life cycle cost. NPV discounts all costs back to a base year so that alternatives can be appropriately compared.

4.1 COST STRUCTURE

This section identifies the cost elements associated with PKI and smart cards. Each agency must determine its actual requirements to forecast the specific cost of PKI/smart cards for the agency. Illustrative examples of costs are provided in Section 8's two case studies. General cost information is provided here.

Figure 4-3: Standard Cost Element Structure

	Year n Constant Dollars Total Costs
Number of New Certificates:	
PROJECT REVIEW	
PLANNING	
Policy Development	
Implementation Plan	
Test & Acceptance Plan	
Bid Evaluation Strategy	
Bidder Communications	
Bid Review	
Award Negotiations	
APPLICATIONS ENABLING	
Program Management	
Toolkits	
Application Upgrades	
Installation/Modifying Applications	
Smart Cards	
Card Readers	
Issuance stations	
Test and Evaluation	
Support	
Upgrade/Product Improvement	
TOTAL APPLICATIONS ENABLING	
OPERATIONAL CAPABILITY	
Program Management	
Concept Exploration (Pilot)	
Training - System Administrator	
Training - End User	
Documentation	
Auditing	
Helpdesk Support	
System Administration	
Vendor Relations Management	
TOTAL OPERATIONAL CAPABILITY	
CERTIFICATE LIFE CYCLE MANAGEMENT	
TOTAL COSTS BY YEAR Constant Dollar	

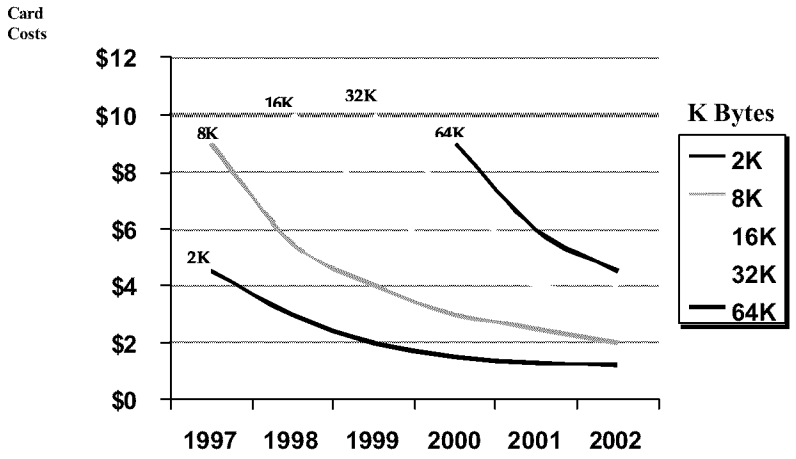
4.1.1 Decreasing Cost

As technologies mature, their costs often drop. This is true of smart card technology, where costs are decreasing rapidly (see Figure 4-4). As usage and acceptance of smart cards have increased, the cost of implementation has decreased. Many agencies buy their cards in bulk to create economies of scale that further reduce the unit cost. One source is GSA's Smart Access Common ID Program. Also, smart cards can be updated without having to reissue the card, creating tremendous cost savings in card stock for issuing organizations.[2]

In recent years, the storage capacity of the card has increased from 2 K to 32 K. Sixty-four Kilobyte cards have been fielded and are expected to be used widely over the next 12 months. In fact, storage capacity on the card has been doubling every 12 to 18 months over the last three years. Additionally, the cost per card has dropped. When initially fielded, many cards cost more than $10; but by the time they were used widely, the price had dropped to less than $6.

2 Based on historical data from major manufacturers in 1997-98 and projected quantities of >1,000,000

Figure 4-4: Decreasing Costs of Smart Cards

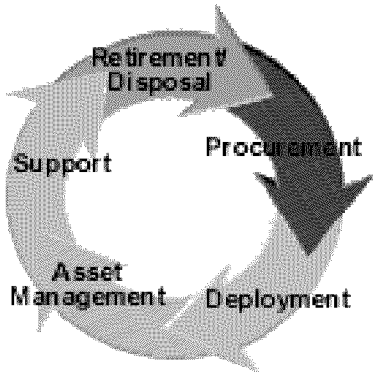


The addition of a cryptographic coprocessor can increase the cost of today's smart cards by 50 to 100 percent. Costs will likely drop as coprocessors become more widespread. In spite of the increased cost, the benefits to computer and network security of including the cryptographic coprocessor are great because the private key can be generated on the card and never leave the smart card.

4.2 COSTS OF PKI

Figure 4-5 depicts the main stages in the life cycle of PKI implementation. Costs for each stage need to be captured.

Figure 4-5: The Life Cycle Phases of PKI Implementation



Because there are both subtle and large differences among agencies, a uniform formula for determining cost of implementing PKI in every agency cannot be recommended. Certain agencies will have the capacity to include the cost of PKI in their IT budgets, while others may not. Some will have the capacity to implement and maintain the PKI with their existing IT personnel, while others will have to outsource such expertise. This will alter the cost of PKI for an agency as well. Some agencies may have the secure facilities that house a CA, while others will have to construct such a facility.

All of the foregoing considerations will alter costs; however, certain common factors have to be considered in computing the cost. For example, the number of Registration Authorities (RA), CAs, and directories that will be required will have to be determined. The factors that affect this decision are the geographical footprint of the agency, the size of the target population, the degree of autonomy of the departments within an agency, etc. The software upgrades and purchases that will have to be made as a result of this implementation also factor into the overall cost.

Another common factor is to decide whether existing IT resources can be leveraged for the PKI implementation and maintenance or whether these will have to be purchased or contracted for. The resource requirements associated with the planning, deployment operation, and on-going maintenance of the infrastructure must be defined. Policies and procedures necessary to support external users or external organizations must also be defined. The results of these and other analyses can help agencies budget for new PKI infrastructure costs as part of the normal IT upgrade budget.

If the PKI is meant to be interoperable, it is essential that a standards-based product and vendor be selected. Without the use of standards, interoperability problems may arise later and would be costly to correct. Liability protection is essential in many cases, especially when interoperability is required with external users or other PKI domains. The need for interoperability with other agencies

Training costs for both end users and administrators may be substantial and will be an on-going cost that declines as the PKI knowledge within the user community increases. Other administrative costs like helpdesk and end entity registration procedures will be on-going and should be included in the cost.

4.3 INCREMENTAL COSTS FOR INCREASED LEVELS OF SECURITY

This section presents a notional example of an agency that is trying to decide what level of security it needs, what are the costs, and what level of benefits can be achieved at each level of security. Four options are presented. This example is based on certain assumptions. They are as follows:

1. Notional agency has 10,000 employees.
2. Physical access requires 1,000 readers and all employees will use cards for logical access. Therefore, 11,000 readers will have to be purchased under Options A, B, and C, which provide physical and logical access. The cost of a physical access reader is $200 under all four options.
3. Cost of infrastructure in this example includes the cost of standing up PKI, the cost of issuing stations, cost of purchasing kiosks, etc.
4. If an agency requires a commercial off-the-shelf (COTS) middleware package, an additional licensing fee of approximately $75 per seat will be incurred.
5. Overhead and program management costs are assumed to be the same for all agencies.

6. The cost of readers, tokens, and infrastructure is based on vendor cost data collection.

4.3.1 Option A—Agency Opts for Magnetic Stripe Cards

Table 4-1 shows the costs of purchasing a magnetic stripe card solution only. Because magnetic stripe cards can be used only for physical access, just 1,000 readers need to be purchased.

Table 4-1: Total Cost of Magnetic Stripe Cards for Notional Agency

Option A - Agency Opts for Magnetic Stripe Cards					
		Unit Cost	Quantity		Total Cost
Cost of tokens	$	0.25	10,000	$	2,500
Cost of network readers	$	200			
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	50,000		$	50,000
Total Cost of Option A (constant dollars)				***$***	***252,500***

As shown in the table, magnetic stripe cards are relatively inexpensive; however, they have a significant drawback in that network access is impossible with this option. Moreover, magnetic stripe cards offer no security features such as nonrepudiation, authentication, data integrity, and confidentiality. Also, the magnetic stripe cards are not upgradeable and are not a highly scalable medium.

4.3.2 Option B—Agency Purchases Smart Cards without PKI

From a functional standpoint, smart cards are better than magnetic stripe cards in many ways. For example, smart cards can store up to 100 times more information in them than a magnetic stripe card. Smart cards lend themselves to a wide range of operations, including financial, healthcare, and transportation. Both physical and logical access are possible with smart cards.

The major drawback relative to this option is that these cards do not have the added level of security that PKI provides. PKI benefits such as nonrepudiation, authentication, data integrity, and confidentiality are very limited with this option. Table 4-2 shows the costs an agency would incur in implementing smart cards without PKI.

Table 4-2: Total Cost of Smart Cards without PKI for Notional Agency

Option B - Agency Opts for Smart Cards without PKI					
		Unit Cost	Quantity		Total Cost
Cost of tokens	$	8	10,000	$	80,000
Cost of network readers	$	50	10,000	$	500,000
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	125,000		$	125,000
Total Cost of Option B (constant dollars)				***$***	***905,000***

4.3.3 Option C—Agency Procures PKI/Smart Cards

With this option, this agency will accrue all the benefits of using smart cards (physical and logical access,portability, upgradeable, and scalability) with the added layer of protection that PKI provides. PKI provides strong data integrity and confidentiality compared with smart cards without PKI. This feature is important because data integrity is critical if sensitive data is stored on smart cards. Of the technologies considered in this report, PKI provides the highest degree of data integrity. Information on the card will remain secure so long as no one has access to the private key. Table 4-3 shows the total costs (in constant dollars) the same notional agency would incur if it chose PKI/smart cards to address business and security needs.

Table 4-3: Total Cost of PKI/Smart Cards for Notional Agency

Option C - Agency Opts for PKI/Smart Cards					
		Unit Cost	Quantity		Total Cost
Cost of tokens	$	15	10,000	$	150,000
Cost of network readers	$	75	10,000	$	750,000
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	200,000		$	200,000
Cost of issuing certificates	$	125,000		$	125,000
Total Cost of Option C (constant dollars)				***$***	***1,425,000***

4.3.4 Option D—Agency Purchases PKI/Smart Cards with Biometrics

Biometrics is the automated procedure for recognizing a person based on a physiological or behavioral characteristic. Examples of biometric identifiers include fingerprints, speech, face, retina, iris, handwritten signature, and hand geometry.[3] Biometrics can be used to either identify an individual as part of a known group or verify an individual against a single biometric. Biometric technology provides a much stronger level of security than PKI without biometrics because it introduces another secure form

[3] Biometric Security: Government Applications and Operations (CardTech/SecurTech Government 1996).

of authentication. This higher level of security is the advantage this option would provide; otherwise, PKI/smart cards offer like benefits.

Table 4-4 shows the cost a notional agency would incur if it implemented a PKI/smart card and biometrics solution.

Table 4-4: Total Cost of PKI/Smart Cards and Biometrics for Notional Agency

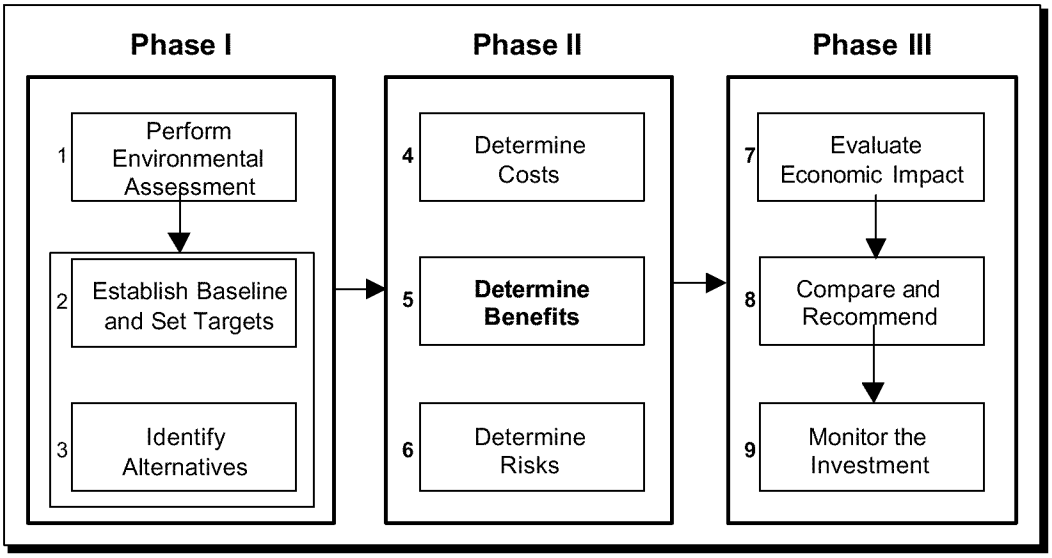
Option D - Agency Opts for PKI/Smart Cards and Biometrics					
		Unit Cost	Quantity		Total Cost
Cost of tokens	$	15	10,000	$	150,000
Cost of network readers	$	125	10,000	$	1,250,000
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	300,000		$	300,000
Cost of issuing certificates	$	125,000		$	125,000
Total Cost of Option D (constant dollars)				***$***	***2,025,000***

4.3.5 Summary

Magnetic stripe cards are the least expensive option; however, they provide no network security. Because a computer is valuable for the data it stores, logical (network) access is important. Clearly, the option with PKI-enabled smart cards is more expensive than either option A or B. However, representatives of many agencies have clearly stated that a high degree of data integrity is required for the information that they plan to carry on their smart cards. In those cases, PKI/smart cards are the best option. The additional protection afforded by biometrics may be required for some agencies within certain departments that require a higher degree of authentication. For other agencies, however, the cost of biometric technology would outweigh the benefits. Given that there are several viable options, an agency has to assess its security needs thoroughly before it can choose which is best given its specific requirements.

5. BENEFIT ANALYSIS

**Figure 5-1: Phase II Determine Benefits—
Business Case Analysis Methodology for PKI/Smart Cards**



Benefits and cost savings/avoidance need to be identified for continuing current operations (the status quo alternative) and for each of the viable alternatives. The business case assumes varying levels of benefits for each alternative in addition to varying costs. To the fullest extent possible, an agency must identify and quantify benefits that will be derived from alternative investments made in implementing PKI/smart cards. Benefits can be expressed as both quantifiable and nonquantifiable (also referred to as qualitative).

- Quantifiable benefits are those that can be assigned a numeric value, such as dollars, physical count of tangible items, or percentage change. Dollar valued benefits comprise cost reductions, cost avoidance, and productivity improvements.
- Nonquantifiable benefits include enhanced information security, consistency and compatibility throughout the enterprise, improved quality, enhancement of best practices, adherence to statutory and regulatory requirements, and enhanced modernization.

Quantifiable benefits are calculated by subtracting the cost of an alternative from the cost of baseline operations. The difference is the “savings” that is often referred to as ROI. Three ways to maximize an alternative's ROI include are minimizing costs, maximizing returns, and accelerating returns. A relatively small improvement in any of the three may have a major impact on the overall rate of return. A sensitivity analysis can be performed to identify the major cost drivers and assumptions and their affect on the alternative's estimated benefits. The sensitivity analysis ensures that all potential improvements and costs associated with using PKI/smart cards within a Federal agency have been captured.

Keep in mind that many benefits realized through an investment will be qualitative and will not lead directly to dollar savings. Improvements in customer service, regulatory compliance, security, and accountability are certainly recognized as benefits, but they rarely can be included in the dollar-valued benefits stream or ROI measures. PKI/smart cards may be difficult to reliably and validly quantify in dollar units, so intangible benefits are vital to understanding the total implementation outcome. These qualitative benefits can be numerically scored by assigning a value to fully meeting, partially meeting, or not meeting stated business or functional drivers. The purpose of this section is to identify the potential benefits of implementing PKI as compared with the potential benefits of implementing smart cards both with and without PKI.

5.1 BENEFITS OF IMPLEMENTING PKI

PKI permits an enterprise to take advantage of the speed and immediacy of the Internet while protecting business-critical information from interception, tampering, and unauthorized access through secure transactions. Proper management and use of public keys enable PKI to provide information assurance and an enhanced operating environment through authentication, data integrity, nonrepudiation, and confidentiality. PKI also offers significant benefits in its interoperability and scalability.

5.1.1 PKI Provides Security Benefits Through Secure Transactions

PKI allows users to communicate securely by offering them controlled access to the intranet for all corporate information, such as human resource data, secure e-mail, and various applications. Unlike other information assurance solutions, PKI does not secure the network or communication link but rather secures the actual transaction through encryption. PKI facilitates the exchange of confidential data with business partners by enabling the creation of secure extranets and virtual private networks (VPN) that give select partners easy access to business-critical information stored on internal networks. Additionally, PKI allows the user to take advantage of secure e-commerce capabilities and helps organizations and companies instill confidence in their customers that they can safely purchase goods and services over the Internet.

5.1.1.1 Authentication. Authentication is the process of reliably determining the identity of a communicating party, or in other words, verifying that a user actually is the one it/he/she claims to be. In the physical real world, a common method of confirming identification is to check a passport, driver's license, ID-card, or similar item. From an e-commerce perspective, it must be possible to verify the identity of the user remotely.

Authentication enables the recipient to determine who actually sent the message and whether that person is authorized to commit his or her organization to the transaction. Additionally, it grants network access to authorized personnel only. Authentication will facilitate a single sign-on capability to access multiple services. Electronic signatures will provide for authentication of online documents for purposes ranging from routing downloads to e-commerce transactions.

5.1.1.2 Data Integrity. Data integrity is protecting against and preventing unauthorized modification of data. Implementing PKI technology will provide for enhanced data integrity. As a result, customers can be certain that data received is accurate and complete, and has not been altered or modified in any manner.

5.1.1.3 Nonrepudiation. Nonrepudiation is the act of verifying the origin and/or issuance of a transaction or action. It ensures that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. It ensures that transactions over the Internet can meet minimum legal standards for electronic commerce and certifies the participants in the transaction.[4]

5.1.1.4 Confidentiality. PKI can be used to encrypt confidential data. Confidentiality ensures that information (e.g., customer data and intellectual property) is not disclosed to unauthorized persons, processes, or devices. Communicating parties can have confidence that data is not viewed, intercepted, or modified by anyone other than the party the message was intended for. Confidentiality is especially important when considering medical data and financial information.

5.1.2 Interoperability

Interoperability can be achieved between two agencies when PKI policies are defined. The security of the PKI technology relies on the protection of the subscribers' private keys. Therefore, recommended PKI solutions will be capable of distributing both certificates and public/private key pairs in a variety of media. Recommended PKI solutions will utilize a single certificate, one that is trusted by all entities, and may be used for multiple agencies or multiple applications thus alleviating the problem of distributing secret keys. This process also simplifies the users registration by decentralizing the registration function. Users who may be strangers to each other can use the CAs to establish a "chain of trust" and interact securely with each other. Building PKI on standards will further promote interoperability.

5.1.2.1 Bridge Certification Authorities. Bridge CAs permit different PKIs to be linked. The bridge CA is a nonhierarchical hub between several participating CAs. All CAs that choose to interoperate with a bridge CA will have the ability to interoperate with each other. The proper use of a bridge CA can demonstrate interoperability on several levels: between CAs, between directories, and between e-mail users. Perhaps the most useful benefit of a bridge CA is that it offers policy interoperability in addition to technical interoperability. Further, agencies can circumscribe risks by excluding certain subtrees that they do not want to interoperate with.

5.1.3 Scalability

The use of PKI technology facilitates "many to many" relationships. PKI enables the use of the same technology for a wide range of applications. PKI creates a trustworthy

[4] Digital signatures provide both nonrepudiation and data integrity.

environment for e-commerce transactions and secure communications over the Internet for both individuals and organizations. The standards-based directory structure can grow as the user base grows.

5.2 BENEFITS OF UTILIZING SMART CARDS

PKI certificates can be stored on smart card tokens. Smart cards have become widely accepted due to the high level of security the card provides compared with PKI certificates stored on a hard drive. Additionally, smart card applications are developed based on standards and using advanced and proven technology. Like PKI, smart card technology also offers significant benefits in its interoperability and scalability, but unlike PKI, also offers portability.

5.2.1 Portability

The small size of the smart card allows for people to carry large amounts of pertinent information on an updateable medium with relative ease. Portability is an important benefit that the small size of the cards facilitates.

5.2.2 Interoperability

Systems can be designed so that a single smart card has the ability to access multiple services, networks, and the Internet. Smart cards have a wide range of applications including, but not limited to, electronic purse, logical and physical access control, healthcare, telecommunications, and transportation. Using a single card to access all of these applications greatly simplifies the logon process for users and administrators alike. Additionally, using the smart card for multiple applications enables cost efficiency to be realized and implementation costs to be shared across the applicable departments.

One way Federal agencies can achieve interoperability with other Federal agencies is through the use of the GSA Smart Access Common ID Program Contract. This contract vehicle can be used by all Federal agencies to acquire a standard, interoperable employee identification card from one or more vendors. In addition to serving as an identification card, the card can also be used for physical and logical (network) access. The Smart Access Common ID card employs several technologies and applications on one card like an integrated circuit chip, magnetic stripe, and digitized photo. In the future, biometrics and other media can be added.

5.2.3 Scalability

Applications can be scaled using smart cards. Smart cards are scalable with regard to the number of users, number of applications, and the number of certificates. This feature permits organizations to expand their smart card usage as necessary without incurring significant additional expenses. Additionally, because some data is shared by applications (e.g., name, social security number, employee ID, address, phone number), these data elements are written once, but read many times. This overlap of data enables organizations to make efficient use of chip space.

5.2.3.1 Users. As the user base grows, more cards and card readers are purchased on an as-needed basis without substantial additional investment expenses. This is due to the fact that the infrastructure is already in place to support the smart card technology and applications. Additional costs will be incurred incrementally and directly related to the number of additional users.

5.2.3.2 Applications. Additionally, smart cards are scalable with regard to the number of applications that can be executed. If there is sufficient chip space available on the smart card, additional applications/functionality may be added. For example, a smart card that is initially being used for stored value and logical access may be expanded to include physical access functionality, chip space permitting.

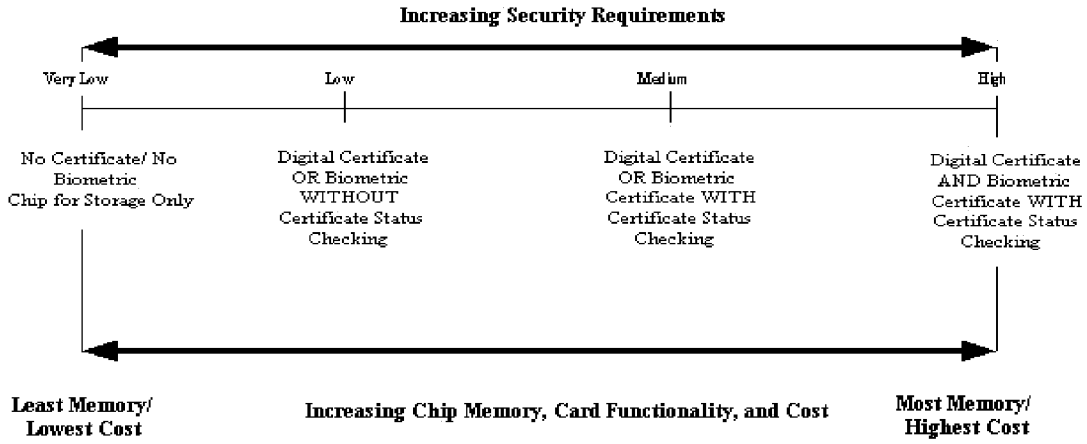
5.2.3.3 Biometrics. The scalability of smart cards also permits organizations to move from a *two*-factor authentication solution to a *three*-factor authentication solution through the use of biometrics. Smart cards can be used with biometrics to provide a verification capability that matches live biometrics scans against a single template that is stored on the chip. Various forms of biometrics can be used for authentication including:

- Facial recognition
- Voice pattern recognition
- Iris scan
- Hand geometry
- Fingerprint recognition

Fingerprint recognition is the most commonly used and cost-effective biometrics solution.

Traditionally, smart cards have been used as part of a *two*-factor authentication system. The first factor is the actual "card," which serves as a token you possess. Secondly, the PIN/password serves as something you know that can unlock secure information stored on the card. A biometrics solution can be used in conjunction with a *two*-factor smart card and PIN/password solution to provide a *three*-factor authentication solution, as demonstrated in Figure 5-2.

Figure 5-2: Greater Information Assurance Through Use of More Factors



5.2.4 Efficiency

Smart cards can be used to complete digital forms (through the population of required data elements stored on the chip) in a more streamlined fashion than their paper-based counterparts, as shown in Table 5-1. A smart card stores pertinent, data such as name, address, social security number, and date of birth, all of which can be used when accessing multiple applications. Using a single card to record and store this data reduces paperwork, eliminates redundant data entry, and improves data accuracy as transcribing and data entry errors are eliminated. Also, ease of use is achieved by using a single smart card for multiple applications. Finally, smart cards enable a higher level of throughput to be achieved because they can process information succinctly and quickly but can also operate in an off-line environment.

Table 5-1: Greater Efficiency via Electronic Forms vice Paper Forms

Paper Forms	Electronic Forms
Increased potential for spelling, transcribing, or readability errors	Core data correctly transmitted from Smart Card
Increased processing time to complete the form	Reduced processing time to complete the form
Increased time to handle, file, and copy the form	Form processed and filed immediately

5.2.5 Data Storage Capacity

The data storage capacity of smart cards is far superior to that of magnetic stripe cards and bar code cards. Most smart cards have a 32 Kbyte chip on which data can be stored compared with a magnetic stripe's storage capacity of about 1000 bits. This capacity permits smart cards to store more than 100 times as much data as magnetic

stripe cards. As a result of their large storage capacity, smart cards working in conjunction with a terminal can execute complex tasks.

5.3 BENEFITS OF IMPLEMENTING PKI-ENABLED SMART CARDS

Although it can be argued that a smart card is not needed to implement PKI, there are some compelling advantages to this security approach. First, it should be noted that all of the benefits attributed to implementing PKI or smart cards also apply to PKI/smart cards. These benefits include:

- Nonrepudiation
- Authentication
- Data integrity
- Confidentiality
- Scalability
- Portability
- Interoperability
- Efficiency
- Data storage capacity.

For the purposes of this analysis, however, the focus is on incremental benefits achieved by implementing PKI/smart cards.

5.3.1 Enhanced Level of Security

The enhanced level of security that can be achieved by implementing PKI/smart cards can be attributed to several factors. One is that the private keys and digital certificates are stored on the smart card. Another is that it provides authentication and encryption capabilities.

5.3.1.1 Private Key Stored on Smart Card. The use of PKI on a smart card can offer an enhanced level of security because private keys can be generated and stored on the card. The much higher level of security is achieved because the non-PKI-enabled smart cards store keys on a floppy disk or hard drive. PKI-enabled smart cards contain an operating system that prevents the keys from being exposed outside the card. Therefore, they cannot be read, removed, or tampered with by anyone.

5.3.1.2 Authentication Using Digital Certificates. PKI/smart cards incorporate cryptographic authentication capabilities that ensure the highest degree of security. PKI/smart cards store digital certificates on the card itself rather than on the certificates on a floppy disk or hard drive, as is the case with other PKI implementations. If stored on a disk or hard drive, a certificate can be copied; but that is more difficult to do if the certificate is stored on a smart card unless the smart card is exploited. A smart card

carrying a PKI certificate makes authentication and nonrepudiation[5] possible by utilizing built-in functionality to accomplish digital signatures. The user carries the card and has a PIN to enable access to use the signature, which is akin to a written signature.

5.3.1.3 Encryption. Encryption capability is a key concern when dealing with sensitive data. Encryption is the transformation of data into a form unreadable by anyone without the proper decryption key. Encryption ensures privacy by keeping the information hidden from anyone for whom it is not intended, even from those who can see the encrypted data.

Public key encryption involves a public key and a private key to mathematically scramble data. While the private key must be kept secure, the public key may be widely distributed. One key is used to encrypt the data, while the other key is used to decrypt it. Encryption enhances the security of data in the following ways:

- Restricts access to your computer to only those users with registered certificates on the workstation
- Verifies the identity of the communicating party through digital signatures
- Ensures that data is stored securely on your computer
- Ensures that files are accessible only by intended parties.

5.3.2 Portability

The portability of private keys and digital certificates is a significant benefit derived from using PKI/smart cards. Because the private keys and digital certificates are stored in the smart card, the user can access the benefits of PKI at any location where he or she is an authorized user.

5.3.3 Scalability

PKI/smart cards are beneficial when they provide a scalable solution. Scalability is advantageous because a public and a private part of keys are involved, and this makes deployment and maintenance of a PKI/smart card easier.

5.4 BENEFITS ACHIEVED BY DOD'S PKI-ENABLED SMART CARD IMPLEMENTATION

One of the largest fieldings of smart cards will begin in December 2000 as the Department of Defense (DoD) begins to implement its PKI/common access card (CAC) on a smart card token to 3.1 million people over the next 2 years. DoD anticipates that smart cards will improve the accuracy, timeliness, security, and cost effectiveness of source data entry and retrieval. The card will be used to improve identification and secure access into physical areas and information management systems.

---

5 The importance of authentication and nonrepudiation is detailed in Section 5.1.

5.4.1 Background

The CAC will replace the DoD Identification Card and be made available to Active Duty, Selected Reserve, National Guard, DoD civilian employees, and eligible contractors. The smart card will contain an Integrated Circuit Chip (ICC) that is read-writable/tailorable as well as any data, applications, PKI certificates, and keys contained on the ICC. The smart card will also include:

- Visual identification (facial photo)
- Printed personal data
- Passive technologies, such as magnetic stripes and bar codes, which carry read-only data or can only be written to a limited number of times.

The CAC will be used to store PKI certificates that provide secure access to web-based, local area network-based, and wide area network-based applications. The credentials stored on the card will replace user login and passwords for individual applications. Private keys and certificates will be used for authentication, digital signature, and e-mail encryption/decryption capabilities.

Smart cards issued in fiscal year (FY) 01 and FY 02 will contain Class 3 PKI certificates. Beginning in October 2002, Class 4 PKI will be put on the card.

5.4.2 Physical Access Control

DoD also plans to use the CAC for access control to facilities. The CAC will provide positive visual verification of the cardholder's identity. The card will be used for proof of identity under all circumstances that a Geneva Convention identification card would be used. The card will provide identification and authentication data that interfaces with existing and future physical access control systems for both secure and nonsecure facilities and spaces.

5.4.3 Logical Access Control

CAC cardholders will be able to securely access public key enabled DoD computer systems and applications at authorized assurance levels. The CAC will be used as a hardware token in combination with a PIN, password, or biometrics so that users can authenticate their identity to public key enabled applications. The card will be an important component of the DoD information assurance vision.

5.4.4 Automated Process

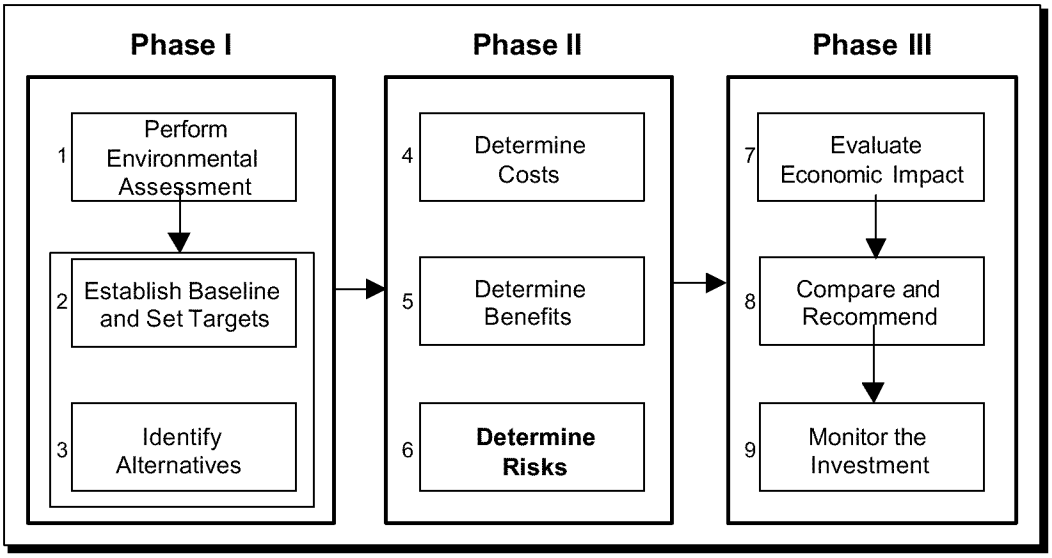
DoD will use the CAC to move from a paper-based, manual process, to a paperless, automated, secure electronic one. This will translate into a higher level of data integrity. Using a single card to record and store this data eliminates paperwork and redundant data entry, and improves data accuracy as transcribing and data entry errors are eliminated.

5.4.5 Cost Reduction

DoD believes the use of smart cards will reduce administrative and logistical support costs as a result of the elimination of paperwork and associated processing time (i.e., labor hours). Documents requiring signature (e.g., travel vouchers) will be digitized, and digital signature will be applied, making the transaction entirely paperless, and yielding tremendous cost savings in processing fees and time.

6. RISK ANALYSIS

**Figure 6-1: Phase II Determine Risks—
Business Case Analysis Methodology for PKI/Smart Cards**



The purpose of the risk analysis is to focus the decision maker's attention on the financial, technical, and schedule risks associated with PKI/smart cards. When documenting your business case, it is necessary to counter-balance positive financial indicators with real-world factors that could potentially undermine your investment and keep it from reaching its estimated potential. This section will help you better understand the risks associated with both smart card and PKI technologies. Risks are inherent to any investment but can be managed to achieve a favorable return on investment.

6.1 RISKS OF SMART CARDS

A smart card is a relatively secure device compared to bar code and magnetic stripe cards. It is a safe place to store valuable information, such as private keys, account numbers, passwords, or valuable personal information such as medical records. It is also a secure platform for performing processes that you do not want exposed to the world, for example, performing an encryption using a public key, or a signature using a private key. Nonetheless, smart cards themselves have inherent drawbacks and risks. These include the high cost of readers, algorithm replacement, lack of standards, loss or theft, and the fact that smart cards are susceptible to many kinds of attacks.

6.1.1 Cost of Readers

One challenge is planning for the cost of card readers. Readers are an essential part of smart card infrastructure as they provide interface between the token and the network. Smart cards can be the basis of trust for secure interaction in PKI for many agencies and their customers. For this to be achieved, a cost effective and acceptable level of

risk must be achieved for all who depend on the associated certificates and keys. Achieving an efficiency of scale between volume of shared PKI-enabled services that use certificates and keys stored on a common token is the desired trade-off. An important element to consider is the high cost of readers. If the smart cards are being used for physical access, contactless smart card readers cost between $200 and $300, whereas contact smart card readers cost between $200 and $400. Acquiring and deploying readers can be challenging, especially where there is substantial legacy equipment lacking that capability. Many computer manufacturers do not outfit computers with card readers; as a result, the additional cost will have to be absorbed by the implementing organization. Targeting incremental deployment of readers associated with the largest evolution of PKI-enabled services has become the key to phased smart card success. Coordination activities with DoD and other agencies may create opportunity to achieve a greater buying power.

6.1.2 Algorithm Replacement

Algorithm replacement is inevitable and as such these replacements and the associated costs will have to be considered at the outset. Algorithm replacement costs and operational impacts to applications and associated smart cards that generate keys should be accommodated through a modular design of algorithm related functions. Every algorithm will inevitably require replacement due to the increasing computer processing capacity (although algorithm useful life can be extended through the use of larger keys. For example, an RSA modulus of 1024 bits is considered secure today; but if it can be attacked within the next 10 years, one solution is to convert to longer key lengths, such as a modulus of 2048 bits). The careful planning for replacement before the anticipated time when an algorithm cannot protect data satisfactorily should be planned into smart card maintenance schemes.

6.1.3 Lack of Standards

Lack of accepted standards within the smart card industry is another drawback. Although smart card readers are standardizing on the ISO 7816 based interface standards, that does not guarantee interoperability with all smart card vendors. Numerous standards exist, and many of them target certain verticals or a certain layer of communications. This leaves out many players. This problem is being mitigated as PKI-enabled Web browsers and other mainstream applications gain the capacity to accept the smart cards and a consensus on basic PKI-based service requests to the smart card. The development of smart card standards, however, is trailing the demands for greater processing and storage capacity on smart cards. By the time standards are developed, the next generation of smart cards is being fielded. To facilitate the ease of use of smart cards in the Federal Government, GSA is assiduously working to establish an interoperability standard. The previously stated buying power that GSA can represent will influence its impact on U.S. Government-unique interoperability standards.

6.1.4 Loss or Theft

Irrespective of the use of the smart card, a primary risk that users face is physical loss or theft of the token. This risk is countered with the inevitable acknowledgement of a missing token and associated revocation procedures to prevent further misrepresentations of the individual's certificate-based trust among associated PKI-enabled applications. A more dangerous risk is theft of keys and discovery of the associated PIN or password used to unlock the keys, without damaging or removing the smart card. This risk poses a far greater threat to the associated trusting PKI-enabled applications and breaches are usually discovered and mitigated only after serious harm occurs, or the certificate is revoked or expires. Regardless of the protections that are built into the system, if the card is not physically protected, laws and security measures will not be effective. This protection is evolving into a combination of user responsibility for physical possession/compliance with associated policies for use and card protection of the keys during generation and/or use.

6.1.5 Attacks on Smart Cards

Smart cards are susceptible to attack by bad actors. An attack is defined simply as an attempt to steal or compromise data on the smart card. There are two classes of attackers—those who are parties to the system, and those who are interlopers. Attacks by participants could be a cardholder trying to cheat a terminal owner, a card issuer trying to cheat a cardholder, or similar behavior. Attacks by outsiders could be mounted via card theft, card misuse, or replacement of terminal software or hardware. Attacks by outsiders are often similar to attacks on protocols involving general-purpose computers; however, they may take advantage of various properties of the system created by the separation of roles. Four kinds of attacks can be made on smart cards: logical, physical, trojan horse, and social engineering.

6.1.5.1 Logical Attacks. One type of attack is logical attack. A logical attack does no physical harm to smart card, rather, some sensitive information on the card is obtained by examining the bytes being transmitted to or from the card. If successful, this attack creates one of the greatest threats (i.e., potential undetected use increases until substantial damage occurs and is noticed). This attack is difficult to achieve because it involves capturing both the private key and associated PIN to perform private key operations. If the byte level I/O operations are monitored, and processing of PKI functions is not performed on the card, both the keys and PIN are exposed.

6.1.5.2 Physical Attacks. Physical attacks are carried out, usually using special equipment, by varying temperature, voltage, or clock frequency, etc., to gain access to sensitive information on the card, or by monitoring card parameters (such as power consumption or the timing of certain card processor operations). Most smart card operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain cleartext keys by directly hacking into the EEPROM. Other physical attacks that have proven to be successful involve an intense physical fluctuation at the precise time and location where the PIN verification takes place. When this happens, sensitive card functions can be performed even though the

PIN is unknown to the perpetrator of the attack. A combination of a physical attack with a logical attack will reveal the private key.

6.1.5.3 Trojan Horse Attacks. A trojan horse attack involves planting malicious code on a user's workstation without the user's knowledge. When the user submits a valid PIN, the trojan horse presents rogue data to be signed using the private key. The user is never aware that the rogue data has been signed. There are two ways of counter-attacking the trojan horse. The first is to use "single-access device driver" architecture. The operating system allows only one "trusted" application to have access to the smart card (if that one application can be compromised, of course, then even this approach can be circumvented). Not using a multiapplication smart card both reduces the number of parties involved and creates a simpler operating environment with less complexity and potential for bugs. Although this reduces the possibility of attack, the benefits to be derived from multifunctionality are, of course, lost. Another way to prevent this type of attack is to require one private key entry per PIN entry; the user must then use the PIN every time the private key is to be used, thereby disallowing the trojan horse access to the key.

6.1.5.4 Social Engineering Attacks. This kind of attack exploits the vulnerabilities inherent in human beings. For example, a hacker could pose as a network technician and request PIN and passwords in order to hack the system. This attack is not as effective when smart cards are involved because people are less likely (or even able) to share their smart card than a PIN or password.

When a decision to proceed with smart cards is made, it is essential to understand that "eternal vigilance" is not only expensive, but impossible. The risks associated with smart card tokens must be understood and bound and balanced against associated benefits. The benefit of cost savings from increased efficiency or compliance should be weighed against the associated threats resulting from the fact that data will be exposed to remote access by users who hold the appropriate PKI credentials. Incremental steps to cost effectively control and leverage the demand for smart cards should be undertaken. The most appropriate system needs for PKI-enabled security services are unique to each set of specified security requirements of an agency.

6.2 RISKS OF PKI

PKI has recently become a popular solution for achieving electronic security and digital-based trust, but it does engender risks that vary in accordance with how the PKI is implemented and what user community it serves. Among the key risks are concerns over the maturity of PKI technology as well as key management itself.

6.2.1 Value Definition

Any PKI implementation should commence with an assessment of what data would benefit from increased exposure that PKI-enabled security services could address. The assessment includes evaluating the monetary or other value of the information and the associated savings that can be realized by allowing remote access. The determination

of appropriate PKI-enabled security services is derived from the associated agency processes and data interchange that could be run cheaper and/or faster, or must comply with Federal mandates (i.e., paperless processes). It is essential to bear in mind that the implemntation of PKI could result in additional exposure of associated data which may not always be desirable.

6.2.2 Lack of Standards

Although in existence for more than 10 years, commercial products implementing PKI technology, have had limited use. Because of its limited use, standards have been slow to emerge. Some PKI standards are not mature or remain defacto because vendors must differentiate their products to justify procurement and the additional cost associated with implementing PKI. Fortunately, this situation is improving due to the efforts of vendor-sponsored organizations like the PKI Forum (http://www.pkiforum.org). However, PKI standards that apply to enterprisewide use of PKI are quite stable. Standards that apply to PKI interoperability are still evolving and have been demonstrated to be sufficient for many applications that require interoperability; but they are not yet ubiquitously or consistently implemented, and thus are likely to evolve further.

6.2.3 Certificate Authority Issues

Among the most critical components of a good PKI is a reliable CA. Without proper certificate authority, the entire PKI process can be compromised. The CA and associated certification practices/policies are the root of trust by which PKI technology is currently deployed. Credibility, represented through the issuance, revocation, and management of certificates, is supplemented by the good will of the issuing agency or service (i.e., how firmly the issuer is willing to stand behind the product). A lack of credibility resulting from poor certicate authority can break the trust necessary for an effective PKI as the CA component provides the trusted binding between a subscriber's public key and his or her identity through the issuance of a certificate.

6.2.4 Registration Authority Issues

The introduction of human error in the RA process presents a risk to PKI. The RA works in conjunction with the issuance process to securely transmit the X.509 data about the individual and validate the identity of the individual when generating certificates, but is not an authority on the contents of the certificates. A human being is required for identity proofing. Sometimes, due to timing constraints, the verifying person may not always be as vigilant as he or she should be. A recommended solution is to require the maintenance of a log of every person identified, recording their name, identification credentials, and time of verification.

6.2.5 Relying Party/Subscriber Issues

- **Root certification substitution**—The root certificate is a certificate self-signed by a CA, containing the CA's public key. The root certificate is usually placed into a browser's trust list of CAs, that is, a list of CAs whom the user wants to trust.

Careful management of this trust list is very important because if a malicious party can surreptitiously place a new root certificate into the list (for a CA that should not be trusted), the user will be relying upon it inappropriately. Thus, centralized management of such a trust list is usually required. In an enterprise PKI, however, only a single root certificate is required—that of the enterprise's "trust anchor" or highest level CA. Managing this approach is much easier because the single root certificate can be placed into the enterprise users' software in such a fashion that malicious alteration of that certificate would be very difficult.

- **Malicious digital signatures**—If a malicious party is able to insert code in a user's computer, he or she can get the user to digitally sign documents or material that the user did not intend to. This can be done without stealing or seizing control of the private key. The malicious code would appear to the user as if he or she is digitally signing something he or she intended to sign. In actuality, the document or material provided to the software that makes the signature occur is actually different from that appearing on the user's screen. However, if a malicious party can insert code in a computer, there is no security approach that will protect the user. Generally, the best way to guard against this type of attack is to protect the user's computer from insertion of malicious code. This however can be difficult to achieve. Furthermore, users should require receipts to be sent for each transaction. Such a protocol makes it very difficult for malicious parties to respond in a timely and effective manner.
- **Name space control**—Certificates contain a public key and the name of the subject to whom the certificate is issued. If that name is ambiguous, such as only a common name, there are opportunities for malicious parties to impersonate the putative holder of the certificate. Additionally, it can be difficult to disambiguate (i.e., distinguish among) the many people who may have the same names as the person cited in the certificate. To minimize the potential for problems, certificates generally should express names using a distinguished naming convention such as that prescribed in the X.500 standard, or that set forth using Internet domain components. An example of the former is "C=US, O=USGovernment, OU=AgencyX, OU=AgencyXsubordinateoffice, CN=Joseph.Smith." An example of the latter is "DC=gov, DC=agencyX, DCN=subordinateoffice, PN=name.agency.gov"
- **Theft of private key and PIN**—If a malevolent party can steal the user's private key (which is usually encrypted) and the PIN or password or other identifier used to decrypt the private key, the user can be impersonated. Doing this, of course, may be very difficult, especially if the private key was generated on and protected on hardware tokens like a smart card. Moreover, such an attack is effective only against the targeted individual—it is not a more generalized attack effective simultaneously against a wide variety of users.

6.2.6 Potential Risk of Implementing PKI

Essentially there are two methods of implementing a PKI; one is to contract for the service and the other is to implement the operation in-house. Both approaches have potential risk, however, these risks are managable. Deciding whether to outsource the

service or implement it in-house must be done not only by comparing costs, but most important, by considering the implementing organization's overall security policy and its requirements. That is, should the agency retain full control of its PKI, or should the agency let someone else execute that aspect of its security? Additionally, an agency must decide if this function is critical to its mission. Government mission critical functions can not be outsourced. Other considerations include the degree of control desired by the agency, the availability of trained staff to implement and maintain the technology, etc.

Although neither way is inexpensive, many companies, lacking sufficient knowledge of security principles, firewalls, and network topologies, find that contracting the implementation is easier. Specialized network engineering firms with trained resources can help setup the network elements and recommend reputable CA firms to handle the PKI authentication process. In any case, a carefully thought-out PKI implementation can help ensure satisfactory operation of a virtual private network (VPN) that assists the business with its goals.

PKI provided in-house from vendors, such as Entrust Technologies, Baltimore Technologies, and Xcert, give an agency greater control. The agency can set its own certificate and key management policies and engineer infrastructure to comply with these policies. In addition, in-house PKI products are more feature-rich, and thus more flexible, than outsourced PKI services.

Outsource PKI services from vendors such as VeriSign, Thawte, and GTE also offer advantages. Costs and schedules are more predictable because the agency can leverage existing expertise. The agency is subject to an outsource PKI service provider's policies but can gain improved interoperability by joining the provider's trust network.

Cost is obviously a concern as well. In-house PKIs cost less per user than outsource PKIs, but overall support costs are higher. Usually, it is expected that an agency will have to issue a significant number of certificates before in-house PKI investment begins to pay off.

A third method of implementing PKI involves procuring services that are customized for the user. The user owns the PKI, but services are provided by a contractor that tailors services to the needs of the owner. This is similar to Government Owned Contractor Operated (GOCO) methodology.

6.2.7 Risks of Digital Signatures

The risks of using digital signatures are broadly covered under three areas: fraud, service failure, and liability.

- **Fraud.** If a person defrauds an agency and a paper signature was used, it is possible in a court of law to prove or disprove that signature. This is not possible with a digital signature. If applied properly, however, the use of digital signatures reduces the risk of fraud. Safety can be assured only if the private key is safe and

not subject to compromise. Creating and storing private keys on hardware tokens (like smart cards) that meet FIPS standards make it more difficult for malicious code to remain undetected.

- **Service failure.** It is important to incorporate electronic services using digital signatures within the scope of an agency's disaster recovery plans. Agencies should also consider establishing backup sites for their CA, RA, and directories that supply the services necessary for applications programs to use certificates.
- **Liability.** As with other interactions that an agency has with outside parties, it has to consider how its actions make it legally liable to affected parties.

6.2.8 Barriers Faced by Agencies in Implementing PKI

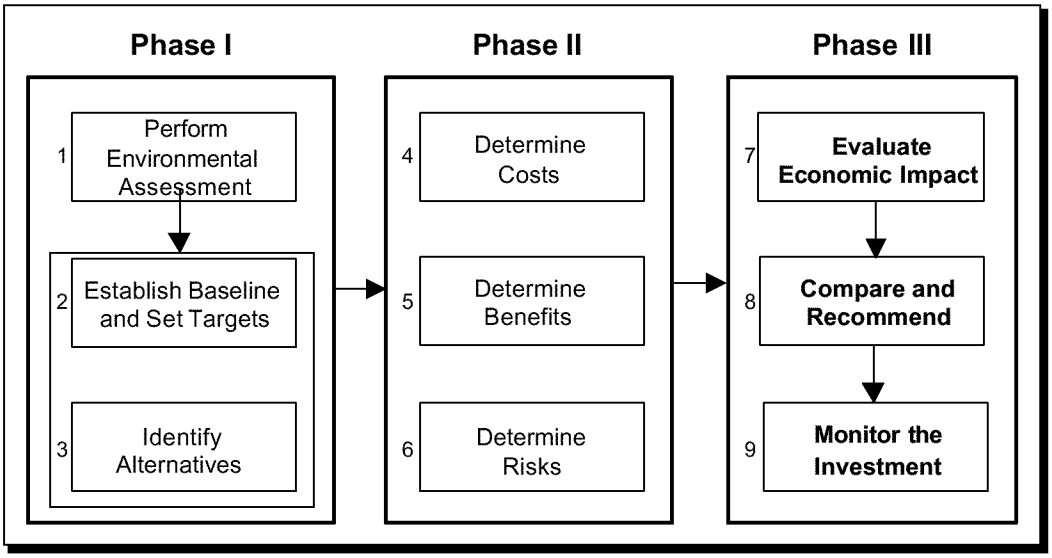
In addition to the risks associated with the lack of maturity of the technology and the fact that use of PKI/smart cards represents a culture shock to some agency employees, there are some other barriers to entry that an agency faces.

6.2.8.1 Infrastructure. Public key infrastructure follows a three-step path to functionality. Step one involves ascertaining that directories are consistent, compatible, and integrated. Step two is the development of procedures to issue certificates that meet accepted standards. Building this infrastructure usually takes a long period of time. Depending on the size of the agency, several RAs may have to be created because they could be distributed. This means procedures have to be taught and certified. Step three is the deployment of the certificates. The complexity of the proccess and length of time required to put the infrastructure in place is often a significant challenge that may be a discouraging factor to agencies.

6.2.8.2 Software Compatibility. In the final analysis, building a PKI provides only an infrastructure but challenges may still exist when trying to interface PKI with existing and future planned applications. How that infrastructure is used is ultimately what interests agency program personnel. Determining how applications programs employ certificates and access the infrastructure to determine whether to trust the certificates requires that applications programs be enabled to accept and use certificates. The process of enablement can be very difficult, depending on which application programs are being enabled, how the agency's directory infrastructure is designed and deployed, and other factors. It is not uncommon that the cost of using a PKI—making applications PKI-aware—can exceed the cost of implementing the PKI itself; although the more applications that are enabled, the greater the utility of the PKI and the long-term savings that are realized.

7. IMPACT OF INVESTMENT

Figure 7-1: Phase III Business Case Analysis Methodology for PKI/Smart Cards



Economic impact can be expressed in one of several ways including cost savings, cost avoidance, return on investment (ROI), payback period or cost benefit ratios. *Cost savings* are reductions in costs compared to those resources actually budgeted for the activity. Realized cost savings are available for reallocation to other activities. *Cost avoidance*, on the other hand, is reductions in costs on activities that were not budgeted therefore the "savings" realized are not available for realloction. In the financial community, the strict meaning of *ROI* is really return on invested capital. ROI may mean simply the incremental gain from an investment, divided by the cost of the investment. In this sense, an investment that costs $1,000 and pays back $1,500 after a short period has a 50 percent ROI. Additonal terms used when conducting a cost benefit analysis includes payback period and cost benefit ratios. *Payback period* is the time period required to fully recover investment expenditures. *Cost benefit ratios* are the ratio of benefit which flow from the original investment compared to the investment expenditure.

The economic impact of an alternative is determined by comparing the total cost of the alternative to the baseline (status quo). When comparing alternatives, it is important to use discounted dollars so that cash flows occurring in different years can be normalized for comparison. Discounted dollars take into account the time value of money that reflects the fact that money in hand today is more valuable than an identical amount of money received in the future. Table 7-1 contains an illustrative example of a cost comparison using cost data presented in Section 5.

Table 7-1: Cost Comparison Among Technologies for a Notional Agency

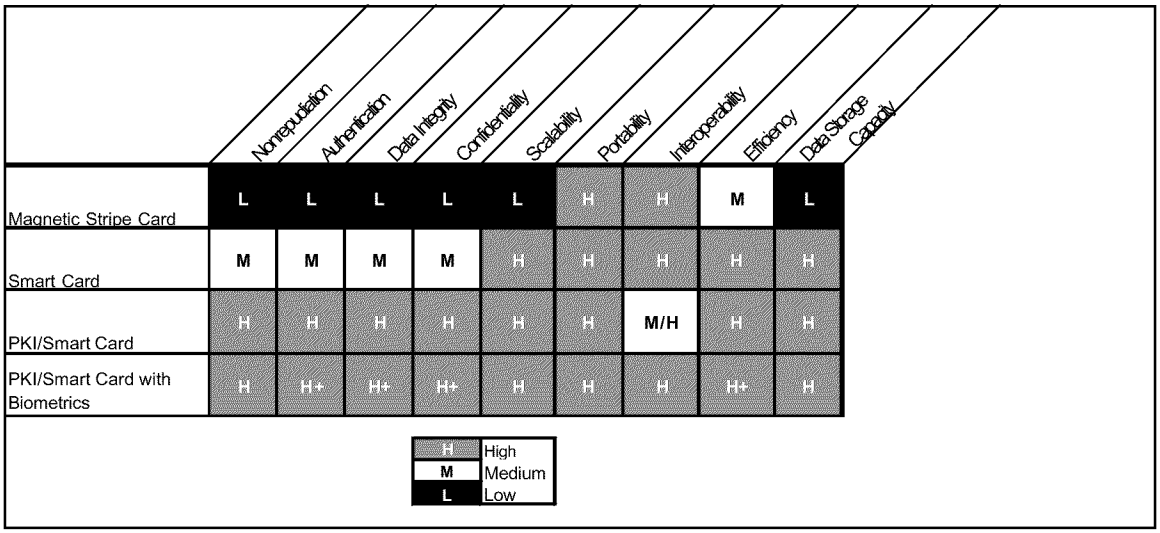
Options	Total Cost
Option A - Agency opts for magnetic stripe cards	$ 252,500
Option B - Agency opts for Smart Cards without PKI	$ 905,000
Option C - Agency opts for Smart Cards with PKI	$ 1,425,000
Option D - Agency opts for Smart Cards with PKI and Biometrics	$ 2,025,000

Additionally, it is recommended that a sensitivity analysis be performed to identify the major cost drivers and assumptions for the alternatives. Conducting a sensitivity analysis also ensures that all potential improvements and costs have been captured.

After the economic impact of each alternative has been established, the alternatives can be compared with one another as well as with the status quo, and an investment recommendation can be formulated. This comparison should include a thorough look at the intangible benefits and increases in effectiveness that cannot be assigned a dollar value. It is often useful to score the alternatives across these criteria so that an objective decision can be made. Alternatives should be compared with one another as well as the baseline. After a thorough comparison of these primary factors, an investment decision can then be made.

Figure 7-2 is a matrix an agency could use to compare benefits across alternatives.

Figure 7-2: Benefit Comparison Among Technologies for a Notional Agency



Ultimately, the business case will serve as the rationale for the selection of a preferred alternative and will contain all of the necessary supporting data and documented assumptions. The business case can then be used to support the budgeting process as dictated by OMB Circular A-11 and provide the basis for managing results for the

preferred alternative, as stated in the Government Performance and Results Act (GPRA).

When the preferred alternative has been selected, approved, funded, and fielded, the agency's job is not over. The investment should be monitored to ensure that it is achieving stated cost and performance goals (e.g., that the investment continues to provide value to your organization.) Some agencies set up performance measures or information assurance security metrics that provide on-going assessments of the value and performance of the investment. Often, failure to monitor the investment carefully leads to less than expected returns. Therefore, it is extremely important to review the investment's performance over the life of the project.

8. CASE STUDIES

The path to implementation of PKI/smart cards by the a large agency and the Federal Deposit Insurance Corporation (FDIC) shows the use of technology, timelines, and reflect the costs that these agencies have incurred. Furthermore, lessons learned are provided at the end of this section to assist agencies as they build their business cases. The two case studies were selected because these agencies have moved beyond the planning phase and are actually implementing PKI/smart card technology. The large agency was selected to represent the path taken by a larger agency with thousands of users. The FDIC was selected to demonstrate an implementation approach taken by a smaller agency with a much smaller user base.

8.1 A LARGE AGENCY

The large organization has three administrations serving approximately 240,000 employees and a large external constituency. The agency has set up an aggressive timeline to implement smart card technology. An internal smart card is meant to be the standard identification card within the agency when interacting with various administrations and offices. The agency's PKI project officially began in 1999 with the CIO Council's endorsement and joint funding by its internal administrations.

The infrastructure is now in place for PKI pilots that support secure e-mail and Web enabled applications for staff and external customers. The agency has outsourced its PKI operations to VeriSign with PKI-enabled Microsoft e-mail and browser clients at the desktop. They use CygnaCom Solutions as the contractor to provide help desk and management support. The agency has issued approximately 1,000 certificates thus far that are in use in various pilots. They will receive 100,000 free certificates from the Customer Advisory Board in FY 2001. In FY 2002, they plan to issue 134,000 additional certificates.

Costs are estimated at $9.1 million in FY 2001 and $72.6 million in FY 2002. The agency hopes to accrue the benefits of cost and time savings and use PKI as a test environment for e-government activities such as those required to comply with the Government Paperwork Elimination Act. Relatively new technology and an aggressive timeline are some of the risks that the agency is facing with regard to this endeavor.

8.1.1 Mission

The implementation of PKI/smart cards promotes the agency mission by:

- Ensuring the confidentiality of highly sensitive information is maintained, especially with regard to medical data
- Providing a means for the constituents to transport core registration data, thus enabling a higher level of service by improving processing time and data accuracy
- Providing strong authentication and digital signature capability to ensure secure data transmission.

Also, smart cards fall within the agency's overall strategy to improve its information security position through strong centralized policy and management and enterprisewide infrastructure capability.

8.1.2 Smart Cards Within the Agency

The agency is in the midst of a plan to implement smart card technology. The smart card will be issued to its employees as well as constituents. For the constituents, this smart card will be the standard identification card for the purposes of interaction with all administrations within the agency.

The agency is currently preparing specifications for the smart card and finalizing the strategy for procuring the necessary software, hardware, and firmware. It is anticipated that a vendor will be selected in late 2000. Other significant milestones include the development of Phase 1–Proof of Concept Demonstration (August 2000); an implementation of a smart card at select sites (January 2001); and finalization of the smart card configuration for the nationally fielded version (January 2002).

There is a smart card management team in place that will guide development of the project and ensure that implementation goals are met and are consistent with stated requirements. The team will guide the life cycle management of the card, develop technical requirements, and determine the budget for smart card use. Also, the agency hopes to implement a tool for the agency to use in re-engineering their respective business practices.

8.1.2.1 Smart Card. The agency is currently in the midst of deploying a smart card. The following are the goals:

- Promote health care versus hospital care
- Seamlessly improve services to constituents
- Reduce data entry errors on records
- Encourage use of electronic business methods
- Implement only one card across the entire agency
- Be honored by all facilities, and all employees
- Will be a scalable card
- Enhance business services and bring inherent value to their mission
- Be network-centric and not card-centric
- Be interoperable across the Federal government and have digital certificate for e-commerce and e-government participation

- Store clinical and administrative data on one card, and be able to change information with ease.

As the card matures, it will be capable of more applications such as:

- Interaction with kiosks
- Prescription refills
- Other administrative purposes.

8.1.2.2 Implementation Plan. The implementation plan covers the management concept of operations, a methodology for requirements planning, a broad communications plan, and an overview of configuration management.

8.1.2.3 Assumptions. The effectiveness of the card is based on the following assumptions:

- Financial resources to obtain hardware and software will be available at the appropriate times.
- Training will be included as part of the initiative.
- Personnel using smart cards are proficient in the use of Windows software and computers.
- Site and implementation managers will work closely to achieve the goals set up for installation and training in the implementation plan.
- Approval of centralized purchase of hardware will be available.
- There will be strong management buy-in and support.

8.1.2.4 Project Strategy. The card will be deployed in three main phases, which are described on the next page.

- Proof of Concept Demonstration
- Initial Implementation
- National Rollout.

Proof of Concept Demonstration. A proof of concept demonstration was performed on August 31, 2000. It demonstrated smart card technology as a viable approach to improving the systems, processes, and data management capability of supporting delivery of care to constituents.

The demonstration was successful, and it was decided to proceed with full implementation of the smart card throughout the agency. The following implementation approaches were adopted as a result of the successful proof of concept demonstration:

- Initial mail-out of cards to avoid long smart card issuance lines at facilities
- Initial implementation at a few sites to begin January 2001
- National rollout to begin no later than January 2002.

Initial Implementation. This phase expands the proof of concept to actual use of smart card technology at two implementation sites. It is expected that business processes, technology configuration, training and communications activities, and support infrastructure will be developed and deployed during the initial implementation phase.

Because the primary goal of the smart card endeavor is to make it easier for constituents to obtain services from the agency, the following factors should be considered in the appraisal of the initial implementation:

- Constituent and staff satisfaction with the administrative and emergency data set
- The card's success in enabling electronic service delivery using public/private key technology
- The success of initial interfaces with existing systems
- Card issuance stations.

Future Plans for a National Rollout. The goal of this phase is to coordinate and support the rollout of smart card technology, including prerequisite hardware and infrastructure verification, software installation, testing, and coordination of training activities and site closeout. Ultimately, PKI/smart cards will be used nationwide.

8.1.2.8 Timeline. The agency timeline is aggressive. The main focus of the smart card project is that it should be an interoperable and integrated solution that can support future uses by the agency and the three administrations. Plans include issuance of smart cards to the target population during calendar year 2001 and to the national target population no later than January 2002. The major milestones of the timeline are depicted in the Table 8-2.

Table 8-2: Major PKI/Smart Card Implementation Timeline

	Task	Start Date	Finish Date
1	Start Smart Card Project	06/27/2000	10/13/2000
2	Workgroup Activities	07/03/2000	04/12/2001
2.1	Express Registration/Eligibility	09/06/2000	02/14/2001
2.2	Emergency Medical Information	08/31/2000	10/18/2000
2.3	Card Issuance and Updating	07/03/2000	10/18/2000
2.4	Physical Design	07/03/2000	10/18/2000
2.5	Communication, Education, Public Relations	07/03/2000	03/02/2001
2.6	Digital Certification	07/03/2000	11/15/2000
2.7	Architecture	07/03/2000	10/01/2000
2.8	Funding and Procurement	07/03/2000	04/12/2001
3	Phase 1 - Proof of Concept	07/03/2000	08/31/2000
4	Phase 2 - Initial Implementation	09/19/2000	10/31/2001
4.1	Pre-Implementation Phase	09/19/2000	11/02/2000
4.2	Site Implementation	01/01/2001	10/31/2001
5	Phase 3 - National Implementation	01/01/2002	02/28/2002
5.1	Pre-Implementation Phase	01/01/2002	02/28/2002
5.2	Implementation Phase	01/01/2002	01/01/2002
6	Closeout	03/01/2002	03/29/2002

8.1.3 PKI Initiative

The agency's PKI project officially began in 1999, with the CIO Council's endorsement and joint funding by its divisions. The infrastructure is now in place for PKI pilots that support secure e-mail and Web enabled applications for staff and external customers. It can expand to accommodate new electronic service delivery initiatives now under development and to accommodate the growing need within the agency to communicate more securely.

The PKI certificate policy has been published. Though this policy will change over time, it is the cornerstone of PKI that will enable orderly expansion, migration to new technologies, and interoperability inside and outside the agency. Information technology and information security professionals were among the first to enroll for PKI certificates, in part to learn what the technology can do and how to use it.

Currently, PKI is used exclusively for secure electronic mail and to provide secure socket layer (SSL) services for some Web servers. PKI subscribers include personnel, contractors, and a few business partners.

A VeriSign on-site CA issues PKI certificates. An LDAP directory managed by VeriSign provides directory services for certificates. Individual certificates may be retrieved from this LDAP directory or shared subscriber to subscriber, and stored in each individual user's e-mail contact list.

Identity proofing is accomplished centrally by personnel and passed through Cygnacom Solutions, Inc. serving as the PKI national registration authority. Cygnacom Solutions,

Inc. also provides documentation and help desk services for PKI subscribers. A Web site is available for PKI subscribers and is updated periodically by the PKI project management staff. This Web site is the portal through which PKI subscribers apply for and retrieve certificates.

Two types of certificates are issued:

- User certificates are attributed to individuals and can be used for secure electronic mail, Web-based applications and remote access services.
- Server certificates are attributed to web servers to provide server authentication and encrypted sessions.

Approximately 350 user certificates and 10 server certificates have been issued through since January 1999. Each certificate is intended for use by employees or contractors and provides secure communication and transactions for internal business processes.

8.1.3.1 Assumptions. The PKI is based on certain strategic assumptions:

- Integrate with security infrastructure
- Outsource CA services for now, but research options further
- Make user certificate repositories publicly accessible
- Keep the number of certificates individuals need to perform business to a minimum—ideally two (one for encryption and the other for signature)
- Use a single source for certificates—and a single policy
- Leverage common Microsoft computing base, but do not wait for release of WIN 2000 to implement
- Coordinate closely with the Enterprise NT effort.

8.1.3.2 Decision to Outsource. The agency currently does not have the required technical expertise to implement and manage a PKI and smart card program. Because this expertise is not the core mission function of the agency, they decided to outsource its PKI and smart card program. Essentially, the agency has placed the liability of key management in the hands of the contractor. The agency wanted to use the GSA ACES contract because it wanted the interoperability that the contract provided. The availability of this contract vehicle reinforced the decision to outsource. The only in-house activities were the bidder communications and some program management.

8.1.4 Costs

Costs of the PKI/smart cards are detailed in the following paragraphs. The cost of the program is expected to be $9.1 million in FY 2001 and $72.6 million in FY 2002.

The agency has deployed some PKI/smart card pilots but most of the implementation will take place in FY 2001 and FY 2002. Therefore, all of the costs shown in this analysis are subject to change and are unfunded as of the publishing date of this report.

Bidder communications and review costs are expected to be $309,101 in FY 2001. Costs of tokens, readers and issuance stations are expected to be $4.2 million in FY 2001 and increase to $60.9 million in FY 2002. Associated costs for testing and evaluation are expected to be $400,000 in FY 2001, and support costs are expected to be $218,510 in FY 2001 and will increase to $700,000 in FY 2002. The upgrades that are expected to occur in FY 2002 are anticipated to cost $2.0 million.

Most of the end user training and system administrator training are expected to occur in FY 2001 and will be $256,000 and $368,000 respectively. Program management costs will be $56,000 in FY 2001, and as the PKI/smart card program expands, program management costs will increase to $2.1 million in FY 2002. Documentation costs are expected to be $450,000 and $1 million respectively in FY 2001 and FY 2002.

Help desk support is referred to as call centers. This support will cost $300,000 and $4.0 million in FY 2001 and FY 2002 respectively. These numbers are consistent with the fact that while some of the program will be implemented in FY 2001, most of it will be implemented in FY 2002.

The agency also has the advantage of being able to use 100,000 free certificates provided by the GSA Customer Advisory Board. Therefore, costs of certificate lifecycle management is expected to be low ($300,000) in FY 2001 and is expected to increase to $1.5 million in FY 2002, when 134,000 additional certificates have to be issued.

The agency decided to outsource all of its activities related to this program except some minimal support activities. Therefore, most costs are outsourcing costs. Table 8-3 shows the costs allocated to the PKI/smart card program over 2 years.

Table 8-3: Total Cost of the Large Agency's PKI/Smart Cards in Constant Dollars

Cost of PKI Enabled Smart Cards

	Year 1 (2001)			Year 2 (2002)		
	In-house costs	Outsourced costs	Total costs	In-house costs	Outsourced costs	Total costs
Number of Certificates:			**100,000**			**134,000**
PROJECT REVIEW						
PLANNING						
Policy Development						
Implementation Plan						
Test & Acceptance Plan						
Bid Evaluation Strategy						
Bidder Communications	$ 109,101	$ 200,000	$ 309,101			
Bid Review						
Best & Final Negotiations						
Award Negotiations						
APPLICATIONS ENABLING						
Program Management		$ 200,000	$ 200,000			
Toolkits		$ 30,000	$ 30,000		$ 330,000	$ 330,000
Application Upgrades						
Installation/Modifying Applications						
Smart Cards		$ 2,431,100	$ 2,431,100		$ 46,350,000	$ 46,350,000
Card Readers		$ 960,150	$ 960,150		$ 5,503,925	$ 5,503,925
Card Issuance		$ 828,000	$ 828,000		$ 9,108,000	$ 9,108,000
Test and Evaluation		$ 400,000	$ 400,000			
Support		$ 218,510	$ 218,510		$ 700,000	$ 700,000
Upgrade/Product Improvement					$ 2,025,000	$ 2,025,000
TOTAL APPLICATIONS ENABLING		***$ 5,067,760***	***$ 5,067,760***		***$ 64,016,925***	***$ 64,016,925***
OPERATIONAL CAPABILITY						
Program Management		$ 56,136	$ 56,136	$ 109,101	$ 1,994,264	$ 2,103,365
Concept Exploration (Pilot)						
Training - System Administrator		$ 368,268	$ 368,268			
Training - End User		$ 256,183	$ 256,183			
Documentation		$ 453,592	$ 453,592		$ 1,000,000	$ 1,000,000
Auditing						
Helpdesk Support		$ 300,000	$ 300,000		$ 4,000,000	$ 4,000,000
System Administration		$ 1,940,264	$ 1,940,264			
Vendor Relations Management						
TOTAL OPERATIONAL CAPABILITY		***$ 3,374,443***	***$ 3,374,443***		***$ 6,994,264***	***$ 7,103,365***
CERTIFICATE LIFE CYCLE MANAGEMENT		$ 300,000	$ 300,000		$ 1,500,000	$ 1,500,000
Total by Year	***$ 109,101***	***$ 8,942,203***	***$ 9,051,304***	***$ 109,101***	***$ 72,511,189***	***$ 72,620,290***

Notes:
1. Received 100,000 certificates for FY 2001 from the GSA Customer Advisory Board. Therefore, Year 1 costs are only transaction fees.
2. In FY 2002, will have to issue 134,000 certificates.
3. One time PKI enabling costs of $200,000 are an approximation.
4. All costs are draft numbers as they are not yet funded and as such, are subject to change.

8.1.5 Perceived Benefits from PKI

The anticipated benefits of the PKI program can be grouped into three main categories.

- **Supports Business Applications.** The project will support real business applications that deliver services electronically over open networks, in particular, the Internet. The benefits of PKI accrue from the delivery of electronic service applications, rather than from the use of PKI in those applications. In other words, PKI creates a trusted environment that promotes the use and growth of all electronic service applications.
- **Cost and Time Savings.** Secure transmission over open networks, for example, could eliminate some requirements for dedicated lines. Electronic forms promise savings from faster processing times, less staff involvement, increased agency responsiveness, and an overall reduced burden on the person submitting the form.

One important aspect of the project will be to permit the quantification of the costs and benefits of using PKI for electronic service applications.

- **E-government Test Environment.** The project provides a controlled test environment within which matters such as customer registration, proofing of identity, mail confirmation, fraud prosecution, liability limitations, compliance with Federal encryption mandates, and Government Paperwork Reduction Act conformance may be addressed.

8.1.6 Risks Related to Successful Smart Card Implementation

The best technology in the world is useful to organizations only if the technology is successfully implemented. The following risks could prevent the successful implementation of smart cards:

- **New Technology.** Compounding the fact that the smart card technology as such is relatively new, is the fact that this is the first smart card project. This factor makes the project risky. Staff and constituents will require extensive end user training.
- **Change.** This relates to change associated with replacing existing business processes and capabilities. To facilitate an effective transmission, clear and definitive guidance must be provided and unilaterally implemented throughout the agency. Also, cultural change and end-user expectations must be managed to include process change, user acceptance, training, etc.
- **Aggressive Timeline.** The agency is trying to implement the smart cards in a very tight timeline (refer to timeline shown previously). This timeline could prove to be difficult to adhere to as it is a relatively new technology, and the concepts have not been fully tested within the agency. The trade-offs however, are cost savings and an improved security posture. The agency decided to proceed with a significant investment in PKI/smart card technology in a rapid fashion so that other electronic commerce solutions could be pursued.

8.1.7 Risks of PKI

Although PKI will be invaluable to the agency, there are some associated risks. Implementing PKI can be an inherently complex undertaking for the reasons explained in the following paragraphs.

8.1.7.1 Extensive Coordination Requirements. The PKI project requires that program, technology, and legal/policy support offices collaborate on a agency-wide approach. Without close coordination across the agency, duplication, gaps and inefficiencies can evolve. Legal, policy, and oversight involvement should also be considered when standing up a PKI/smart card infrastructure.

8.1.7.2 Inexperience With PKI Technology. Although PKI has a firm theoretical underpinning and a growing spectrum of applications, its use represents unexplored territory for most of the agency. The policy and technology framework for PKI does not

exist, so it must evolve from a pilot experience. Customer registration and proofing, liability, fraud protection and prosecution, and record privacy and preservation are among the issues that need to be addressed. There is also the need for flexibility as the underlying technologies evolve and become more standardized.

8.1.7.3 Internet Self-Service Context. Self-service over the Internet requires an agency to understand customer demographics and preferences, and revisit the rules and traditions that apply to in-person and mail contacts. Certain policies and procedures must uniformly govern all electronic service applications.

- The requirement to provide for a customer to “opt in”
- Notification by mail of all updates to an individual’s record
- Procedures to notify customers of agency's and the customer’s respective responsibilities and limitations on liabilities.

8.2 THE FEDERAL DEPOSIT INSURANCE CORPORATION

The Federal Deposit Insurance Corporation's mission is to maintain the stability of and public confidence in the nation's financial system. FDIC has about 7,800 employees.

FDIC generated its first certificate policy and certification practices statement in 1998. The FDIC's Electronic Travel Voucher (ETV) system was its pilot program. ETV currently makes use of encryption and digital signature technology. FDIC has issued 3,500 certificates in FY 2000 and plans to issue about 5,000 more in FY 2001 to complete the PKI enabling within the corporation.

In addition, FDIC is using Entrust profiles on Datakey 320 smart cards. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration. FDIC also implemented secure extranet applications using digital certificates for FDIC external clients. This is a low assurance PKI used for authentication purposes only. FDIC maintains the PKI in-house because it will be used for the core functions of the agency. FDIC spent $5.0 million in FY 2000 and plans to spend $2.5 million in FY 2001.

FDIC is currently working on developing a high level Application Programming Interface (API) to make it PKI consistent irrespective of which PKI product is used. This will facilitate the development and wide-deployment of PKI-enabled applications. This is explained in detail in Section 8.2.4.

Table 8-4 provides the FDIC mission and vision statements. The FDIC has insured deposits and promoted safe and sound banking practices since 1933.

Table 8-4: FDIC's Mission and Vision Statements

FDIC Mission	"The FDIC, an independent agency created by Congress, contributes to stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships."
FDIC Vision	"To assure that the FDIC is an organization dedicated to identifying and addressing existing and emerging risks in order to promote stability and public confidence in the nation's financial system."

The implementation of PKI/smart cards promotes both the FDIC mission and vision by:

- Addressing potential risks due to security breaches
- Ensuring only authorized personnel gain access to sensitive data
- Improving the ability to track and detect suspicious activity across FDIC systems
- Ensuring the confidentiality, integrity, and availability of its information are maintained.

8.2.1 Background

FDIC has successfully combined picture identification badges with smart card chips mounted on the badge. The badges, controlled by the security office, are issued after an employee has participated in the FDIC personnel security program. Unlike a generic token, these are registered to a specific user. To implement these badges, a product search was undertaken that was limited to those devices capable of operating within the FDIC's PKI. Datakey 320 smart card chips were selected and have been tested. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration.

Following pilot testing, it is expected that FDIC will begin using smart cards for all high-risk electronic transactions that require a digital signature. A new Datakey 330 smart card chip is expected to be available after it has undergone Federal Information Processing Standards (FIPS) 140-1 level 2 verification. When this technology is combined with a picture badge, the FDIC will be able to satisfy user cryptographic requirements associated with General Accounting Office (GAO) authorization.

8.2.2 Low Assurance PKI

FDIC uses a low assurance PKI for a number of SSL Web-based applications on its extranet with its member institutions and other parties that are external to the agency, such as other state or Federal agencies. Browser certificates are used to control access to the extranet Web server. The extranet PKI uses a 128-bit RSA encryption via SSL, and employs Entrust WebCA software. The extranet PKI currently has about 2,000 certificates issued and is from the medium assurance PKI. The extranet uses software-based protection mechanisms (Web browser certificates). It provides authentication only.

8.2.3 Electronic Travel Voucher System Pilot

FDIC has approximately 3,500 field representatives with laptops. All field representatives will have to use ETV to get reimbursed. The electronic system is interfaced with the National Finance Center (NFC). Previously, it took up to two months for field employees to be repaid, but after the implementation of smart cards it now takes two days for a direct deposit to reach the employee's account. The paper reimbursement process used to cost about $50 a transaction to process, whereas the new process costs less than $10. FDIC processes about 80,000 to 100,000 vouchers every year. This results in savings of about $3.2 to $4.0 million.

In addition to quantitative advantages such as cost savings, qualitative advantages to using the ETV include:

- Quality of data check
- Expedience of service
- Reimbursement is a direct deposit to the checking account.

ETV uses digital signatures and some encryption. Although the transition to PKI was a significant change for the employees, the expedience with which they are reimbursed has led to this technology being welcomed by the field representatives. As a result of the success of the ETV pilot program, FDIC has expanded the program to a fully operational, on-going cryptographic smart card endeavor.

8.2.4 PKI Enabling Within FDIC

FDIC generated its first certificate policy (CP) and certification practices statement (CPS) in 1998. Development of the version 1 policy took approximately 1 month and underwent OIG review. FDIC is planning plans that future development and revisions should last no more than 3 months. A single CP[6] is being generated to address four assurance levels. This will use the DoD CP as a template. FDIC is reviewing the Federal Bridge Certificate Policy for cross certification purposes. Each CA will have a Certification Practices Statement (CPS).[7] Each of the assurance levels will have a separate certificate profile. Specifically, the approach is to use Federal Information Processing Standards (FIPS) 140-1 validated hardware cryptographic modules for the CA. High assurance digital signatures will also become part of the smart card capabilities.

Through a competitive bid process, FDIC selected the firm Entrust as its PKI provider. Within FDIC, the PKI is run internally (not outsourced) and managed by the people who manage the issuance of passwords. The current architecture consists of an Entrust Manager (version 3.0c1) and an ICL X.500 version 7B Directory Service. The client software that is deployed to the user is the Entrust Client v3 for desktop users and Entrust Entelligence v4.2a (with Entrust ICE/ True Delete/ Secure Delete) for the laptop users. The infrastructure is currently being upgraded to Entrust Manager v4, with the hopes of increasing it to Entrust Authority (version 5) very soon. Additionally, the hosting CA platform will support a FIPS 140-1 level 4 cryptographic module to contain the CA signature keys, once upgraded.

Entrust provides free toolkits that enable the Secure Communication Manager (SCM) to interface with high level cryptographic Application Programming Interface. SCM is an FDIC developed middleware application that is intended to reduce the complexity of the

6 A Certificate Policy is a registered set of rules on the applicability of a certificate.

7 A Certification Practices Statement details and controls the certification process from the initial verification of the institutional requestor and the request for certificate process, through the issuing, acceptance, using, suspending, revoking, and renewing of certificates.

underlying mechanisms while facilitating service requests through simple service calls. The SCM was modified to recognize hardware tokens.

The FDIC is working with other government agencies in defining a high-level API that would work with developed government off-the-shelf (GOTS) applications. This interface will be PKI consistent regardless of which PKI product is used. This will facilitate the development and wide deployment of PKI applications and will make support across multiple PKI products less difficult. FDIC has established links with the Department of Energy, Department of Treasury's Financial Management Services Division, NIST and GAO. FDIC has also had some contact with the Environmental Protection Agency and feels that the Department of Army may show interest.

Certain client software upgrades need to be made before migrating to Entrust 5.0 Manager. FDIC is testing the build for a corporate desktop upgrade that will bring everything up to version 4.X. FDIC is also procuring the software necessary for establishing a full PKI for the Extranet. FDIC will shadow the internal directory to the extranet Border Directory and cross certify with customers. FDIC expects to cross certify with the Federal Bridge CA at the low assurance level using this interface.

Phase 1 of the PKI enabling will involve 2,500 examiners who are in the field most of the time. These examiners need assurance that there is only one key set, but this cannot be accomplished with a floppy disk that can be copied, whereas it can be accomplished by a smart card. The issuance of smart cards will be coordinated with the badge issuance office. The badge issuance vehicle will also be the issuer of smart cards.

Phase 2 will include the rollout of PKI on all desktops. Currently, this phase is expected to commence in early 2001.

The smart card will also be used for physical access except in places where office space is leased and it may not be possible. In other staffed access controlled areas where the badge is presented to the reader, it actually scans the image of the bearer of the card and provides physical verification to the guard. Although there is no secure compartmented information facility (SCIF)-like secure area within FDIC, FDIC personnel feel that one should be created where the CA is housed. There are still areas within the FDIC where five-button security (cypher locks) will continue to exist.

8.2.5 Program Management and Support

Program management and support are on-going throughout the lifecyle of the project. These program management activities include the following:

- Training
- Help desk
- On-going maintenance
- Audit

Training within the FDIC is an on-going process based on a "train the trainer" model. FDIC has numerous help desk facilities. The Entrust specific help desk is located at the large agency and is staffed with contractors from Computer Associates. Users, information security officers, and field office representatives are given a toll free number to contact if any operational issues arise with the Entrust environment. The on-going maintenance contract FIDC has with Entrust is its Silver program, which costs 18 percent of the contract value per year. Administrators and government oversight personnel perform auditing to ensure contract compliance.

8.2.6 Certificate Life Cycle Management

The on-going certificate lifecycle management process is clearly defined within the FDIC and is explained in detail below.

8.2.6.1 Certificate Issuance. The core users have been issued certificates. The FDIC opted to develop an automated registration tool to support the ETV rollout. In contrast, the use of smart cards will eventually require a human in the loop to issue a key because FDIC will use High assurance cards that require a human validate the cardholder.

8.2.6.2 Certificate Renewal. Certificate renewal is automated within Entrust. The certificate policy specifies the validity period. When the certificate nears expiration, it is automatically renewed unless explicitly denied.

8.2.6.3 Certificate Distribution. Certificates are distributed within the Entrust product to the client. Encryption certificates populate the X.500 directory and the signature certificates are concatenated with the signature of the CA.

8.2.6.4 Certificate Backup and Recovery. The Entrust Manager is backed up daily. Recovery requires RA intervention. The RA must establish that the user is whom they claim to be. There is also an information security officer reporting system that is used to make recovery requests.

8.2.6.5 Testing and Maintenance. New software versions must be tested in lab and test environments. Older versions of the software are not supported by the vendor and therefore need upgrading.

8.2.7 FDIC Timeline

FDIC was able to successfully complete PKI enabling of its pilot project at the scheduled time. It plans to roll out PKI/smart cards to all its employees and some contractors by March or April 2001. FDIC had planned to complete the rollout by January 2001, but a delay in deploying Windows 2000 software had delayed the full implementation by a few months. As explained earlier, FDIC has decided to keep the PKI endeavor in-house and has not contracted out any portion of it. FDIC has established the tentative timeline shown in Table 8-5 for implementing PKI/smart cards.

Table 8-5: Major FDIC PKI/Smart Card Implementation Timeline

	Task	Timeframe
1	Needs Study	January 1997
2	Low Assurance PKI	January 1998
3	Certificate Practices	August-September 1998
4	ETV Decision	Early 1998
5	ETV Cut Over	December 1999
6	Issuance of 3,500 Smart Cards	November 2000
7	Full rollout of Smart Cards	March-April 2001

8.2.8 Decision to Not Outsource

The crux of FDIC's decision to not outsource relates to the future vision for PKI/smart cards. FDIC will use smart cards for its high dollar value obligations in the future. Such a critical and core function should not be outsourced to an outside vendor because the potential for significant losses is high. By keeping this function in-house, FDIC retains control of the function and can take appropriate steps to protect against losses.

The other deciding factor was that a GAO sanction will not allow for this core function to be outsourced, and FDIC is obtaining this GAO sanction. Because many financial obligations will be made with digital signatures, it can be expected that the GAO will become involved. The concern is that data integrity could be compromised. GAO will sanction only a high level of assurance that will require a person in the loop for face-to-face identification.

8.2.9 Costs

Thus far, the cost of PKI enabling within FDIC has been $1 million for the program management of the infrastructure alone. The $1 million does not include CA contract support, FDIC contract support or government personnel time.

The costs of planning and project review were not assigned to the PKI/smart cards endeavor. Rather they were subsumed in the overall operations cost of the agency.

As an agency, FDIC had the advantage of being able to roll up the costs of hardware with its enterprisewide laptop upgrade. Only the costs for the tokens and the readers were assigned to the PKI/smart cards project. This meant that the only costs were those for standing up the PKI, which was $1 million in program management costs. FDIC created the middleware called SCM, so it did not incur the license fee (approximately $75/seat) that can substantially add to the costs.

The ETVS pilot, which has been described in detail previously in this report, cost approximately $2.75 million to stand up. All of these costs were incurred in FY 2000. The cost of issuing cards and readers was $357,000 for approximately 3,000 tokens

and is expected to be $678,300 in FY 2001 for approximately 5,700 tokens. A one-time testing cost of $100,000 was incurred in FY 2000.

Ongoing help desk support that is staffed by contractors from Computer Associates is expected to be approximately $300,000 for the first two years when the PKI/smart cards are being put in place. When proficiency has increased, helpdesk costs are expected to decline. System administration, including auditing and training, is expected to require three FTEs and have a recurring cost of approximately $300,000 per year. Ongoing maintenance is provided under the Entrust Silver program, which is 18 percent of program management costs or approximately $200,000 each year throughout the life cycle of the project.

Table 8-6: Total Cost of FDIC's PKI/Smart Cards in Constant Dollars

	Year 1 FY 2000 Total Costs	Year 2 FY 2001 Total Costs
Number of New Certificates:	3,000	5,700
PROJECT REVIEW		
PLANNING		
Policy Development		
Implementation Plan		
Test & Acceptance Plan		
Bid Evaluation Strategy		
Bidder Communications		
Bid Review		
Award Negotiations		
APPLICATIONS ENABLING		
Program Management	1,000,000	1,000,000
Toolkits		
Application Upgrades		
Installation/Modifying Applications		
Smart Cards	66,000	125,400
Card Readers	291,000	552,900
Issuance stations		
Test and Evaluation	100,000	
Support		
Upgrade/Product Improvement		
TOTAL APPLICATIONS ENABLING	***$1,457,000***	***$1,678,300***
OPERATIONAL CAPABILITY		
Program Management		
Concept Exploration (Pilot)	2,750,000	
Training - System Administrator		
Training - End User		
Documentation		
Auditing		
Helpdesk Support	300,000	300,000
System Administration	300,000	300,000
Vendor Relations Management	200,000	200,000
TOTAL OPERATIONAL CAPABILITY	***3,550,000***	***800,000***
CERTIFICATE LIFE CYCLE MANAGEMENT		
TOTAL COSTS BY YEAR	***$5,007,000***	***$2,478,300***

Notes:

1. Planning and project review costs were not direcly assigned to the PKI Smart Cards project.
2. Certificate life cycle management is part of vendor relations management costs.
3. Year 1 costs include the cost of the ETV pilot, which is $2.75 million.

8.3 LESSONS LEARNED

These two case study candidates demonstrate that it is possible to implement PKI/smart cards irrespective of the size of the agency. Although there is currently no uniform methodology of implementing PKI/smart cards, there are three different methods that an

agency can use. An agency can either outsource the activities as the large agency did with VeriSign or decide to conduct all the operations in-house like FDIC decided. The advantages and drawbacks of both have been discussed. A third method involves a government-owned/contractor operated type ownership, where a user owns the PKI, but a contractor provides customized PKI services. This method was not used by either case study candidates.

8.3.1 Benefits Versus Risks

Both the large agency and FDIC were aware of the general risks posed by use of PKI and smart cards and the obstacles to successful implementation. However, these agencies believe that the benefits outweigh the risks and have, therefore, proceeded with the implementation of cryptographic smart cards. In fact, discussions with agency personnel from both the large agency and FDIC reveal that they believe there is no better option for security available and that implementing PKI/smart cards is an inevitable decision.

8.3.2 Costs Versus Benefits

Both the large agency and FDIC incurred substantial costs in implementing PKI/smart cards. The incremental costs of each added layer of security should be analyzed against the extra benefit that the added security feature provides. Both the large agency and FDIC used PKI to enhance their security and realize higher levels of authentication, data integrity, nonrepudiation, and confidentiality. These agencies also purchased smart cards due to the added benefits of portability, scalability, and interoperability. Although biometrics technologies offer a higher level of security, both agencies felt that the currently high costs of biometrics readers makes this option not feasible for now.

8.3.3 Preparing for Implementation

The implementation of PKI/smart cards infrastructure requires significant planning and consideration throughout your agency. Below is a checklist of some of the important factors that your agency should consider before implementing cryptographic smart cards. This checklist is distilled from literature review and is based on lessons learned from case studies and interviews with both PKI and smart card subject matter experts.

1. Prepare a Certificate Policy and a Certificate Policy Statement

A certificate policy is a bare minimum requirement that has to be prepared before operating a PKI infrastructure in a disciplined environment. A certificate policy will provide the map for your agency's business model for electronic transactions. Additionally, a certificate policy statement should be prepared if your agency is going to operate its own certificate authority (CA) or have a contractor operate the CA on behalf of the agency. This certificate policy statement defines the operating procures for your CA, namely, key management.

2. Determine Your Agency's Need for Interoperability

If your agency has a high need to transact business with other agencies, the Federal Bridge Certification Agency (FBCA) is a very efficient mechanism to provide the interoperability required for this interface. The advantage of linking with the Federal Bridge is that you enter into one certificate management arrangement with the bridge and have access to all other Federal Bridge users rather than having to draft bilateral agreements with every agency with which you conduct business. If your agency chooses to operate with the FBCA, it should consider the certificate policy of the bridge in framing your own certificate policy. Additionally, the GSA Smart Access Common ID Program contract is a means of obtaining interoperable smart cards that can used between agencies.

3. Consider Phasing In Implementation

Discussions with agencies about their PKI enabling efforts indicate that it is more practical to adopt a phased in approach to PKI. This incremental implementation allows your agency to learn from and deal with any mistakes you may make in the pilot process and allows for the scaling up of such activities as program management and helpdesk capabilities. It also allows the cost of implementation to be spread over more than one fiscal year, which could prove beneficial in securing necessary funding.

4. Departmentwide Implementation and Policies

The substantial infrastructure investment and on-going certificate issuing costs of PKI suggest that a departmentwide approach be taken to achieve centralization of infrastructure and economies of scale. The substantial marketing efforts that will be required to establish incentives and to encourage adoption of PKI digital signatures by users and constituents suggest that a centralized marketing campaign would be more effective and economical. A number of commonalities could exist among agency functions and users that will have to be established. Although each agency has a different mission, the commonalities would suggest that a unified approach could be taken to meeting information security requirements. Several PKI solutions are being tested in pilot projects within specific departments that use certificates from several vendors. It is possible that any PKI applications going forward can be met by an enterprise approach to PKI within each department. The same is true of smart cards, as all agencies within a department could issue the same smart card with the same amount of memory.

5. Define the Registration Process

Your agency may decide to incorporate your certificate registration process into the existing personnel or facility office business practice of issuing identification cards. For most agencies, the smart card will replace identification cards; so this step is really streamlining PKI into an existing business process, resulting in a nominal cost impact to your agency. For example, when a new employee is hired, the subscriber agreement

that is required to obtain a digital certificate and a smart card can be part of the rest of the hiring package. The smart card can be issued as part of the normal in-processing.

6. Establish a Certification Revocation Policy and Validation Procedures

Several options are available to establish certification revocation policy that disables certificates if the smart card is stolen or inoperable, or when an employee terminates. The revocation of certificates ensures that security remains intact. Two common certificate revocation approaches are Certificate Revocation Lists (which is the most common today) and the Online Certificate Status Protocol (OCSP) approach of "Validation Authority." One key decision that should be made in establishing the revocation policy is how stringent the policy will be. A very stringent policy leads to a number of revocations, while a less stringent policy results in fewer revocations. It is extremely important for your agency to put in place validation procedures, expired certificates procedures, and Certificate Revocation Lists. Also, your agency should decide who has the responsibility of providing long-term signature validation services.

7. Forecast Liability Issues

Your agency should determine up front what liability, if any, it will assume for failures in the certificates it issues and under what conditions it will assume such liability. It may be better for your agency to posit the use of PKI as a method of preserving trust rather than creating trust.

8. Determine Use of Smart Card

A smart card has several potential uses, including physical access, logical access, electronic purse, transit cards, and medical information storage. Every agency will not require every one of these functions. Therefore, an agency needs to consider how the smart card is to be used in support of its mission and vision. An agency could first implement a card with a few applications and add additional applications after the intial set of applications are deemed stable; however, it is important at the outset to develop a vision for how the card will be used both in the near-term and long-term. This allows agencies that plan multiple applications to buy smart cards with the appropriate amount of memory at the beginning so that new cards will not have to be issued later. Rather, the new application can simply be added to the existing card thereby reducing reissuance costs.

9. CONCLUSION

PKI/smart cards are a sound business investment when they are used to satisfy security and business needs as they provide the means for secure online transactions. Compared to other technologies, PKI/smart cards offer tremendous security benefits through the encryption of transactions using PKI to offer nonrepudiation, authentication, data integrity, and confidentiality. By placing PKI certificates on a smart card, scalability, portability, interoperability (via the Federal Bridge), efficiency, and data storage capacity are possible. PKI/smart cards can be used for logical access to computer networks as well as physical access to buildings.

This report was prepared as a means of helping Federal agencies understand the components for building a sound business case for using PKI/smart cards within Federal agencies. By following the business case methodology presented in this document, decision makers will be able to determine for themselves whether the investment costs for PKI/smart cards are justified and whether the benefits outweigh the risks. Decision makers are also given guidance on evaluating the economic impact of alternatives, comparing alternatives, and ultimately monitoring the investment.

An environmental assessment will demonstrate whether PKI/smart card technology is well suited to improve the security posture of an organization; to achieve legislative, executive, and agency guidance compliance; to enable an agency to accomplish its mission; and to support e-government initiatives. Many baseline business processes in use today include identification cards, magnetic stripe cards used for physical access, and PIN or password technology for logical control. The use of PKI/smart cards will change these processes. Several technologies that can address an organization's security and operational needs include static, upgradeable, and cryptographic smart cards. However, PKI/smart cards offer a tremendous benefit compared to other technologies. In fact, only PKI yields a high benefit in the security areas of authentication, nonrepudiation, data integrity, and confidentiality. Agencies that require this level of security benefit are most suitable candidates for this technology.

In a notional agency of 10,000 users, the cost of PKI/smart cards hardware is shown to only be about $142 per user (excluding the operational and maintenance costs required to operate these systems). PKI/smart cards can complement planned IT upgrades as part of an overall IT investment rather than assigning the full cost of implementation to the PKI/smart card project. ROI calculations help to make equitable comparisons of alternatives to the status quo by evaluating their individual economic impact. Cost alone should not be the sole basis of an investment decision but rather a composite of factors like benefits, risks, and costs should be evaluated. When an alternative is selected, it should be fully documented in a business case that details the entire selection process. After the investment is made and the preferred alternative is fielded, the investment should be monitored for actual performance against targets.

Two case studies illustrate two separate but successful paths Federal agencies have taken to implement PKI/smart cards. The case study example is of a large agency that will use PKI/smart card technology to service both internal and external users. Being relatively inexperienced in key management, large agency decided to outsource its PKI management. FDIC is a smaller agency that will use PKI/smart card technology to interface with other agencies and corporations. FDIC has decided to manage its own PKI. Both agencies used pilots to test proof of concepts before deploying. These "real world" examples help to demonstrate that PKI/smart cards can be a sound investment for secure transactions.

APPENDIX A
ACRONYMS AND ABBREVIATIONS DEFINED

ACES	Access Certificates for Electronic Services
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BCA	Business Case Analysis
CA	Certificate Authority
CAC	Common Access Card
CIO	Chief Information Officer
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
DoD	Department of Defense
EBCDIC	Extended Binary Coded Decimal Interchange Code
e-business	Electronic Business
e-commerce	Electronic Commerce
EEPROM	Electrically Erasable Programmable Read-Only Memory
e-government	Electronic Government
e-mail	Electronic Mail
ETV	Electronic Travel Voucher
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FY	Fiscal Year
GAO	Government Accounting Office
GOCO	Government Owned, Contractor Operated
GOTS	Government off the Shelf
GPEA	Government Paperwork Elimination Act
GTE	General Telephone & Electronics
IA	Information Assurance

ICC	Integrated Circuit Chip
IRR	Internal Rate of Return
ISO	Industry Standards Organization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NASA	National Aeronautics and Space Administration
NCA	National Cemetery Administration
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NPV	Net Present Value
OCSP	Online Certificate Status Protocol
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
ROI	Return on Investment
RSA	Rivest, Shamir, & Adleman
SCIF	Secure Compartmented Information Facility
SCM	Secure Communications Manager
SSL	Secure Socket Layer
VPN	Virtual Private Network

APPENDIX B
GLOSSARY OF PKI AND SMART CARD TERMS

Access	Ability to make use of any information system (IS) resource.
Access control	Refer to logical access control and physical access control.
Access Certificates for Electronic Services (ACES)	ACES provides secure electronic access to the Public for privacy protected Federal services and information through the use of public key technology
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Availability	Guaranteed service on demand assurance
Biometrics	Refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.
Byte	8 bits
Certificate	A digital representation of information that at least (1) identifies the Certificate Authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the Certificate Authority issuing it.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines the transformation of plaintext data into ciphertext data; the transformation of ciphertext data into plaintext data; a digital signature computed from data; the verification of a digital signature computed from data; or a data authentication code (DAC) computed from data.

Cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Data Integrity	Provides absolute verification that data has not been modified or tampered with.
Digital signature	A method of encryption that provides authentication, nonrepudiation, and data integrity.
Efficiency	In this analysis, efficiency includes productivity gains realized from automation, time savings, and convenience.
Encryption	The translation of data into a secret code.
Form factor	The physical size and shape of a component.
Government Paperwork Reduction Act (GPEA)	GPEA allows citizens to use electronic technologies when filing information with, or retrieving it from the Federal Government. GPEA provides the legal framework for agencies to accept electronically submitted forms and documents. Electronic signatures and other measures will be used to authenticate citizens as they transact business with the Government.
Government Performance and Results Act (GPRA)	GPRA requires agencies to define missions, set goals, measure performance, and report on their accomplishments. As such, an agency's IT investments should directly support the accomplishment of these goals.
Hardware	The physical equipment used to process programs and data in a cryptographic module.
Integrity	Refer to data integrity.
Interface	A logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.
Interoperability	The ability of software and hardware on different machines from different vendors to share data.
Kilobyte	1,024 bytes (abbreviated Kbyte)

Logical Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Non-repudiation	Nonrepudiation is the act of assuring the origin and/or issuance of a transaction or action.
Password	A string of characters used to authenticate an identity or to verify access authorization.
Personal identification number (PIN)	A 4- to 12-character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.
Physical access control	Refers to access to buildings.
Portability	Can be carried or moved with ease.
Privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity and not made public.
Presidential Decision Directive (PDD) 63	PDD-63 required Federal agencies to secure critical infrastructures against terrorist attacks.
Public key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public.
Public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that given the public key, it is computationally infeasible to derive the private key.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Scalability	Refers to how well a hardware or software system can adapt to increased demand.

Token	The cryptographic module associated with a given user for PKI and common access card functions. It includes private keys and associated public key certificates, identification data, and other information relevant to these functions. This is not to be confused with a token device such as a smart card, which may contain a token but is not in itself considered a token.