Appendix E

Public Key Infrastructure at the Department of Justice

White Paper

Appendix E
Public Key Infrastructure White Paper*

Introduction

As part of its strategic plan, the Department of Justice (Department) is seeking opportunities to improve many facets of its operations. The Department is faced with many different obligations in meeting its responsibilities. Since the terrorist attacks of September 11, 2001, the Department has been asked to take a larger role in the war against terrorism. At the same time, the Federal Government has urged its departments and agencies to conduct their business functions electronically to the extent possible while insuring information security. The Government Paperwork Elimination Act (GPEA), in particular, encourages the use of electronic documentation and electronic signatures. In accepting these additional responsibilities and improving its business processes, the Department has identified significant shortcomings in its abilities to meet these demands.

Traditionally, each component within the Department has been responsible for managing its own information technology (IT) infrastructure. This has led to disparate systems that cannot communicate with each other. Therefore, the Department has identified the need for a unified IT architecture with the ability to do the following:

- Securely access applications owned by other Department components
- Conduct much of the Department's routine business electronically, within the Department, with other Federal agencies, and with the public (e-government)
- Provide State and local law enforcement personnel access to Department applications in the execution of their roles and responsibilities

The Department has identified a minimum set of required security services that must be provided by the unified architecture to meet the growing reliance on information services. The following minimum security services must be available across the Department's IT infrastructure:

- Confidential (i.e., encrypted) information exchange
- Information integrity
- Strong authentication
- Digital signature and non-repudiation
- Advanced key management including key escrow, long-term key archive, and efficient key revocation
- "Litigation-strength" security
- Operation across different environments, allowing the secure interchange of information at multiple information sensitivity levels with external trading partners, other Federal agencies, Department components, and the public.

Cryptographic functions such as encryption and secure hashes can help protect the information. However, many of the challenges of meeting the Department's goals are associated with verifying the identity and authorization of individuals attempting to access the Department's information. Application administrators need a mechanism to verify an individual's authorizations before granting them access to system resources. Individuals must authenticate

* This White Paper is based on unpublished material prepared by SRA for the Department of Justice.

themselves to each application. If each application uses a separate password for authentication, then the individual must remember each password. When faced with the necessity of remembering many different passwords, individuals will typically use easy to remember passwords, use the same password for all systems, or write down the passwords. All of these pose significant security threats to the Department's information.

Public key technology can assist the Department in providing a secure, unified, information technology infrastructure that will meet these goals. Public key encryption may be used to implement digital signatures, secure hashes, and encryption services. This technology is based on using two discreet keys, a public key and a private key, to perform the cryptographic functions. The private keys are safeguarded by the individual who will sign or decrypt the messages. The public key is made available to other users to verify the signature, or encrypt messages for that particular individual.

Requirements for a Department-wide Public Key Infrastructure

A Public Key Infrastructure (PKI) provides the supporting mechanisms necessary to use public key cryptography. The primary components of a PKI are the certificate authority (CA) and registration authority (RA). The CA issues certificates to individuals that link their private and public keys together. It provides the trust mechanism so that individuals and applications can have assurance that a particular public key is associated with a particular individual. Certificates also can define specific authorizations or capabilities that a user may possess. Individuals are enrolled in the system by a RA.

Since there is a significant overhead cost associated with establishing and securing the key elements of a PKI, this technology has been adopted slowly by the Government and industry. However, it offers the greatest promise of meeting the Department's long-term IT security goals of providing a unified, secure IT infrastructure throughout the Department. As e-government progresses and more Government agencies and departments implement their own PKI solutions, the Department will need to interact electronically with citizens, businesses, and other Government entities. For example, the Federal judiciary has begun implementing an electronic case file (ECF) system that eliminates paper documents at the court. Although the ECF system is not currently using a PKI, it is envisioned that a PKI solution will be necessary as the ECF is migrated from the civil sector to the criminal sector. As the courts move to a paperless environment, the Department's attorneys will also need to move in that direction.

A Department-wide PKI will enable the following:

- Confidential (i.e., encrypted) information exchange between authorized individuals
- The implementation of strong (two-factor or more) authentication mechanisms
- Digital signature and non-repudiation capabilities
- Trusted authentication across organizational barriers within the Department, with other Federal departments, with State and local law enforcement organizations, and with the public. A single authentication method for users across multiple applications, reducing

the number of password-related help desk calls resulting in direct cost savings to the Department

By providing a mechanism for strong authentication and the verification of digital signatures, a PKI can enable the Department to migrate many of its manual processes to electronic mechanisms. A PKI can provide the needed trust to enable e-government and e-commerce to materialize, with their potential cost savings and improved workflows. The interface with other law enforcement departments and agencies will provide the ability to better coordinate resources and conduct investigations.

The following section highlights some potential benefits of developing a Department-wide PKI. Annex 1 lists some of the currently identified PKI initiatives within the Department. Annex 2 identifies some potential applications that can be developed using the Department-wide PKI. While any of the applications listed in Annex 2 may be implemented without a PKI, they would each need to establish and manage separate authentication schemes. Individuals who use more than one application would need to employ a different authentication mechanism for each application. The Department-wide PKI would provide a common authentication scheme that all applications could use, allowing individuals to use a common authentication mechanism for access to all applications for which they need access.

Department-wide PKI Benefits

The Department has already begun several PKI initiatives. All PKI efforts within the Department have been initiated to meet a specific operational requirement. They reduce paperwork associated with fulfilling legal mandates, automate workflow process, or provide improved authentication. The majority of these initiatives have focused on requirements within an individual component with only limited cross-organizational PKI efforts. A list of currently identified PKI initiatives within the Department is provided in Annex 1.

A Department-wide PKI will provide the following direct benefits to the Department:

- The ability to establish timely and secure electronic communications
- Cost savings associated with automated work processes and reduced help desk calls
- Additional cost savings with a centrally-managed PKI solution over multiple component-level solutions

The Department has a growing reliance on electronic information. There is also increasing pressure for better coordination within the Government in the war on terrorism and crime in general. These factors will require all of the components within the Department to exchange information with other components and agencies securely.

A Department PKI would provide many benefits to the Department. One of the administrative activities the Department-wide PKI could support is the automated processing of travel vouchers, forms, and leave requests. Electronic processing would reduce errors and increase the efficiency in processing these routine reports. An early Department PKI cost/benefit analysis estimated an

annual savings of nearly $29.5M by automating the work flow process. Potential future applications that could benefit from the Department-wide PKI are listed in Annex 2.

Additional cost savings may be possible with fewer help desk requests to reset forgotten passwords. If users are able to use a single authentication mechanism for all accesses, then users will be less likely to forget or write down their passwords.

The Department may develop a centrally managed PKI solution, or allow each component to develop its own solution and provide a bridging capability between the components, the Federal PKI Bridge, and other entities. The development and maintenance of several CAs and building a bridge between them may be more costly than building a single, larger CA. Additional savings would be made in only developing a single certificate policy (CP) and certificate practice statement (CPS), instead of duplicating this development at each of the components. Developmental costs would be focused on one system rather than several. Administration costs would also be lower to support a single CA, rather than several.

The bridge approach would provide more autonomy to each of the components and would not provide a unified infrastructure. Each component would need to go through the expense of implementing and maintaining separate CAs. Access control modifications to component applications also would need to accept certificates from other component CAs. All of the Department's shared services would need to accept certificates issued by any of the components' CAs. This would be a difficult undertaking.

The need for interoperability along with the potential cost savings[1] indicates the need for a centrally-managed Department CA. The limited number of skilled personnel available for Federal and contractor support also indicates that the Department's efforts be consolidated.

A central Department CA would provide a unified infrastructure that would be consistent across all components. This would allow application access modifications to be accomplished in a standardized manner. It would also allow the Department to consolidate the costs of implementing and maintaining the PKI. Each component would still retain control over their information and could also take on the RA activities and responsibilities.

Some components may have unique security requirements that dictate that they have their own PKI and provide their own certificates. However, these components will need to securely communicate with other components and others outside of their PKI. The Department-wide PKI would support the administrative and functional activities of the agency by providing a framework to allow the components to securely communicate across organizational boundaries. Without a central Department-wide PKI, each component will need to cross-certify CAs with each organization it needs to communicate. The Department must consider any perceived security benefits along with the increased cost of implementing multiple CAs and a bridge CA.

[1] A formal cost analysis was not completed as part of developing this white paper.

Appendix E
Public Key Infrastructure White Paper

The Department PKI Program Management Office

To implement a Department-wide PKI, a program management office (PMO) will need to be established. The PMO will lead the effort to establish a common PKI throughout the Department. It will also serve as the interface with other Government PKI initiatives.

The PMO responsibilities can be divided into several functions: Architecture, Audit, Infrastructure and Shared Services, Operations, and Policies and Standards.

Architecture

The PMO will be responsible for developing the overall PKI architecture. The architecture will define how each of the components will be integrated into the PKI and how external agencies, law enforcement, and the public will be incorporated. Also, since the PKI will be a critical service for the Department, contingency plans must also be considered when designing the architecture.

The Department-wide PKI would also provide a conduit to State and local law enforcement agencies. Figure 1 shows the conceptual architecture. The conduit would provide a path of trust so that certificates from the Federal, State, and local law enforcement agencies could be accepted by each other. This capability would be useful as multiple agencies try to coordinate investigative activities that cross jurisdictional boundaries. Through the use of the Federal Bridge CA, individuals would be capable of securely communicating with individuals from other branches of Government. This is especially important as the Government focuses its resources on specific functions. The country's fight against terrorism, for example, requires that individuals from many different Federal, State, and local departments and agencies collaborate securely.

Some key questions that will need to be considered are:

- Who will be responsible for registering individuals?
- What backup and recovery plans will be implemented?
- How many redundant certificate servers will be used?
- How will the components access the certificate servers?
- How will law enforcement access the certificate servers?
- Will hardware tokens or biometrics be required?
- Who will be required to use them?
- Can different tokens or biometrics be used in different portions of the PKI?
- What electronic services will be made available to the public?
- Will the public services make use of the Department-wide PKI? If so, How?

Appendix E
Public Key Infrastructure White Paper

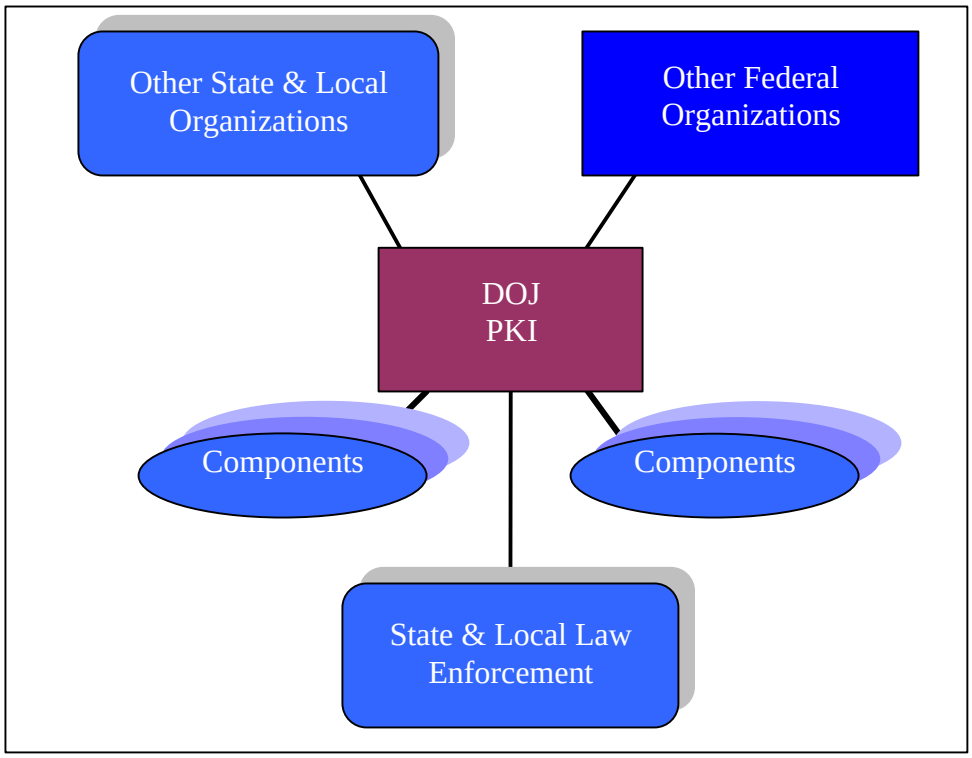

Figure 1. Department-wide PKI Concept

Audit

Since the PKI provides critical security services to the Department, it is important that it be maintained securely. The audit function will verify that necessary security precautions are implemented to protect the CA, RA, and other critical PKI functions. Audit activities would include the following activities:

- Reviewing audit logs
- Performing a formal annual audit of the CAs and RAs
- Evaluating the effectiveness of security controls
- Conducting the initial and subsequent certifications and accreditations of the PKI systems

Infrastructure and Shared Services

The Department's infrastructure must also be updated to accommodate the PKI services. Server, network, and backup capabilities must be able to handle the demands that will be placed on them. Also, the Department's shared services will need to be integrated into the PKI. The PMO will need to ensure that the total infrastructure is PKI-ready and that the shared services are PKI-enabled. Activities would include the following:

- Enabling PKI in shared applications
- Identifying necessary enhancements to the Department infrastructure

- Establishing a Department directory service
- Defining the physical security requirements for PKI elements

The Department currently provides some shared services to multiple components. Some of these are listed in Table 1. By sharing these services, the Department is able to reduce the total cost of establishing and maintaining these services. The PMO would be responsible for providing the necessary PKI services for these shared services to continue to reduce the total cost of establishing and maintaining these services. This would provide a mechanism for implementing strong authentication mechanisms throughout the agency.

JCON – Justice Consolidated Office Network – desktop and e-mail (Exchange) services
JOIN – Justice Online Internet Network – Internet, intranet, and browser services
JUST – Justice Message Service – store and forward message service. Primary application is to provide Federal law enforcement personnel access to the FBI's National Crime Information Center.
Justice Automated Messaging Systems – provides a secure messaging system service. Smaller components would rely on the Department's PKI for support.

Table 1. Department Shared Services

The greatest benefit of establishing a Department-wide PKI will be the ability to communicate securely across organizational boundaries without requiring a complex verification and validation process. The Department-wide PKI will facilitate the secure communication between individuals in separate components, throughout the law enforcement community, and with other Government departments and agencies.

Operations

The PMO will be responsible for establishing the operational procedures for the CA, RA, and other components of the PKI. Maintaining the confidentiality, integrity, availability, and accountability of the certificates is a critical function of the PKI operations. Some activities include:

- Issuing and maintaining public and private keys
- Issuing and maintaining certificates
- Registering individuals
- Issuing tokens
- Revoking certificates
- Verifying certificates
- Maintaining PKI servers
- Escrowing encryption keys

Policies and Standards

The PMO will also establish the policies and standards for interoperation with the PKI. The policies and standards will define the various levels of access that may be granted and the requirements for individuals and organizations to be enrolled at given levels. These policies and standards will need to address Department personnel, law enforcement personnel, and any other individuals who may need to gain access to Department resources. The Department also needs to consider the legal ramifications of implementing a PKI and using PKI-protected information in a court of law. Some of the policies that will need to be developed include the following:

- Trust levels
- Legal constraints
- Key retention
- Physical security
- Registration requirements
- Cross-certification policies
- Hardware token policies

The Department is participating in the Federal PKI Steering Committee which provides Government-wide guidance and coordination of Federal activities to implement a Federal PKI. One of the major tasks of this committee is the establishment and management of a Federal Bridge Certification Authority. This Bridge CA will support secure communications and commerce between Federal agencies, other branches of the Federal Government, State, and local governments. It allows other Federal CAs to accept certificates from other organizations by providing trust levels for the participating CAs based on their policies.

In order to allow the Department PKI to serve as a conduit to the Federal Bridge and other CAs, the Department would take the following actions:

- Continue its involvement with the Federal Bridge program
- Define an architecture for sharing certificates
- Provide standard Department-wide directory services
- Develop a Department CA policy and procedures
- Implement a Department CA
- Connect to the Federal Bridge

Next Steps

To be successful, the Department needs to modify its business practices and establish the importance of implementing a Department-wide PKI. A Department PKI PMO would be responsible for establishing the Department-wide PKI and leading all Department PKI activities. This office also would be responsible for developing and implementing the security functions of the Department-wide PKI, such as establishing the Department-wide policies and procedures and

developing the conduit to other organizations' CAs. Some of the PMO activities would include the following:

- Developing funding and cost estimates
- Updating the Department Security policy to reflect PKI and Digital signatures
- Developing a Trust Model
- Providing Department-wide directory services
- Developing a unified information infrastructure
- Developing a Concept of Operations (CONOP) for the PKI
- Developing Certificate Policy (CP)
- Developing Certificate Practice Statement (CPS)
    - Defining the RA process, including the need for tokens or biometrics
    - Developing key management procedures
    - Defining individual responsibilities
    - Developing backup and contingency plans
- Defining deployment goals
- Developing deployment roadmap
- Making infrastructure modifications – upgrade systems, install new equipment for the PKI, smartcards, readers, physical environment, etc.
- Developing PKI pilots
- Implementing PKI-enabled services
    - Implementing the pilot
    - Training users
    - Rolling-out the PKI-enabled system

PKI Pilots

An essential part of implementing a successful PKI is implementing a pilot program and then migrating the technology throughout the Department. The Department-wide PKI pilot programs need to focus on applications between different components and across the Government. The programs would focus on those technologies that will provide the greatest benefit to Department users. Four of these are: secure e-mail, virtual private networks, user authentication, and web-based applications.

Secure e-mail. PKI-enabled e-mail would allow the greatest flexibility in providing secure electronic communications. An initial pilot would focus on intra-Department secured e-mail between different components. This capability would then be applied throughout the Department on a phased basis. After successfully piloting an intra-Department solution, the Department might then focus on interagency pilots to promote secure communications with other Government and law-enforcement organizations.

PKI-enabled Virtual Private Network (VPN). PKI-enabled VPN access to Department resources would allow the Department to consolidate and control its telecommunications expenses. Remote users currently dial into the systems that they need to access. A VPN would

allow the Department to consolidate telecommunications resources and provide greater security for remote users. This scenario could potentially provide a cost savings as well. A pilot would begin with a single component and then be migrated throughout the Department.

Strong User Authentication. The Department-wide PKI would be used as part of a strong authentication scheme. Users would be required to use at least two factors to authenticate themselves to the system. The Department-wide PKI would focus on the shared services and enable them to use the hardware token or biometric information as one factor in the authentication process.

Web-based Application Security (Single Sign-on). One of the Department's security goals is to provide a single sign-on capability for Department applications. Currently, the easiest manner to accomplish this is through a web interface. Web applications can be PKI-enabled to recognize the Department-wide PKI. Users would then only need to authenticate to the PKI which would validate the user for each web application. The PMO would need to identify web-based applications that would benefit from being PKI-enabled. Legacy applications would need to have a web front-end in order to include them in the single sign-on environment.

In addition to establishing the Department PKI, the Department PMO would lead the law enforcement PKI community of interest (COI) panel. This panel would work with the Federal PKI Steering Committee to establish mechanisms for the interoperability of PKIs used in law enforcement. Some of the activities of this panel include the following:

- Establishing a Community of Interest Panel
  - Reviewing business requirements, legal framework, and cooperative policies
- Defining identity framework within Community of Interest (COI)
  - Defining how to identify levels of confidentiality, availability, integrity, and authorization, such as a layered approach to meet business, legal, and policy requirements
  - Considering larger interoperable security framework into other sectors
- Developing CA and RA requirements

Summary

The Department is being asked to conduct more of its business electronically, both internally and externally with other Government agencies and the public. Due to the current war on terrorism, individual components need to work more closely with each other and with other law enforcement organizations. A Department-wide public key infrastructure could aid the Department in providing timely and secure electronic access to information and in implementing e-government.

References

Paperwork Reduction Act of 1995 (44 USC 3501-3520).

Appendix E
Public Key Infrastructure White Paper

Government Paperwork Elimination Act (Title XVII of P.L. 105-277). 1998.

Memorandum for the Heads of Executive Departments and Agencies. Subject: Electronic Government. Dec 17, 1999

Department of Justice Information Technology Architecture Public Key Infrastructure Cost Benefit Analysis. October 1999.

The Evolving Federal Public Key Infrastructure, Federal Public Key Infrastructure Steering Committee. June 2000.

Federal Agency Use of Public Key Technology for Digital Signatures and Authentication (NIST Special Pub 800-25, October 2000).

An On-going Assessment of Government Information Assurance, e-Business Policy, and Implementation in a Changing 'Trust' Environment – A Potentially Disruptive Technological Approach. Federated Electronic Government Coalition, May 3, 2002.

Appendix E
Public Key Infrastructure White Paper

Annex 1: Current Department PKI Initiatives

The Justice Management Division (JMD) has initiated two PKI efforts. The first prototype is the Secure Encrypted Title III (SET3) PKI initiative involving the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). The purpose of this program is to increase the effectiveness and efficiency of personnel supporting Special Agent operations by enhancing the confidentiality, authenticity, integrity, availability, and reliability of the Title III Pre-Authorization Approval Sub Process (PAASP). Participants who request, and respond to requests, regarding Title III Electronic Surveillance records are able to sign and encrypt e-mail documents.

The second initiative was a civil PKI prototype that is no longer in use. The prototype involved encryption and digital signature support for the civil law environment. The preliminary participants were the Department's Tax Division and the Internal Revenue Service (IRS). Both e-mail messages and desktop files were encrypted and signed.

In addition to the JMD-initiated efforts, individual Department agencies have developed PKI initiatives to meet specific requirements. Some of these initiatives are presented in this section.

The FBI has identified two PKI initiatives. The first is to develop an FBI-wide internal PKI system that would be used for creating and managing Virtual Case Files (VCF). They have also implemented a PKI-enabled application to allow Federal Firearms Licensees (FFL) to request a search of prospective firearms purchasers through an FBI web site.

The DEA's Office of Diversion Control is using two separate pilots as a proof of concept for meeting the regulatory requirements associated with controlled substance prescription and distribution. The first pilot is being conducted with the Department of Veterans Affairs and focuses on the benefits that a PKI-enabled system might provide in prescribing and dispensing controlled drugs from a pharmacy. The second pilot involves manufacturers and distributors and is attempting to reduce the paperwork burden associated with manufacturing, transporting, and distributing controlled substances.

The DEA also uses a PKI to allow secure remote dial-in access to Firebird, the DEA's office automation network.

The Immigration and Naturalization Service (INS) has implemented a PKI to provide limited e-mail security and file encryption. It also issues certificates to INS web servers to enable them for Secure Sockets Layer (SSL) connections. INS also uses a PKI to support laptop encryption.

Annex 2: Potential Applications Using the Department-wide PKI

By providing a mechanism for strong authentication and the verification of digital signatures, a PKI will enable the Department to migrate many of its manual processes to electronic mechanisms. A PKI can provide the needed trust to enable e-government and e-commerce to materialize, with their potential cost savings and improved workflows. The interface into other law enforcement departments and agencies will provide the ability to better coordinate resources and conduct investigations. This section highlights some potential applications that might be developed using the Department-wide PKI.

While any of these applications may be implemented without a PKI, they would each need to establish and manage separate authentication schemes. Individuals who use more than one application would need to employ a different authentication mechanism for each application. The Department-wide PKI would provide a common authentication scheme that all applications could use, allowing individuals to use a common authentication mechanism for access to all applications for which they need access.

Employee Access

Mobile and wireless computing devices can be PKI-enabled. This would provide the future capability of granting secured access to e-mail and other electronic information through devices such as a Personal Digital Assistant (PDA). Information on the laptop or other mobile computing device may be encrypted or otherwise protected with the PKI to prevent unauthorized access if the device should be lost or stolen. Traveling employees must also be able to securely communicate while conducting investigations, preparing court papers, or performing other tasks away from the office. The Department-wide PKI would permit the Department to provide VPN access to Department resources from virtually any location. This could potentially provide a cost savings as telecommunication links are consolidated.

With a common infrastructure, employees could be assigned to different components and offices within the Department without having to modify all of their information. As needs arise, individuals with the appropriate skills may be placed on task forces or other assignments without regard to which component they work for primarily.

Federal Government Communications

Employees gain access to their pay and benefits information through the National Finance Center (NFC). By integrating the Department-wide PKI with the Federal PKI, employees will be able to use the same Department token to access their personnel information. The authenticity and non-repudiation factors might be extremely important as employees reallocate their Thrift Savings Plan funds and the markets fluctuate.

Law Enforcement Community of Interest

The Department must also communicate with other Federal, State, and local authorities. By establishing PKI standards for the law enforcement community, certificates may be cross-certified and allow secure information sharing at all levels of law enforcement. The FBI has already established a program to allow Federal Firearms Licensees access to FBI data to conduct checks for potential firearms purchases. The FBI, INS, DEA, and other components could

provide services to the law enforcement community. This same technology might expedite the process of searching for outstanding warrants when individuals are arrested. This also would enable multiple agencies to securely communicate with an ad hoc command center when responding to high-profile crime scenes such as the World Trade Center.

Contractor Communications

PKI provides the ability to conduct business electronically. Although this aspect of PKI is less mature than other uses, the Department might eventually take advantage of its PKI program to manage its contractors. Contracts and Task Orders could be issued electronically with digital signatures. Contract deliverables also could be encrypted, signed, and delivered electronically. The NFC has already implemented a PKI for conducting e-commerce.

Public Communications

The General Services Administration's Access Certificates for Electronic Services (ACES) program facilitates secure access to Government information and services by the public. This program would allow the Department to provide secure services to individuals who have a valid ACES Certificate.

The Department also publishes public information on Internet web servers. The Department may digitally sign the contents of the web pages and then periodically validate that they have not been modified inappropriately. If an attacker were able to modify any of pages, then the verification process would detect the change and could take additional actions.