NIST Special Publication 800-25

Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Kathy Lyons-Burke

Federal Public Key Infrastructure Steering Committee

C O M P U T E R S E C U R I T Y

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director
- National Quality Program
- International and Academic Affairs

Technology Services
- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program
- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program
- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory
- Biotechnology
- Physical and Chemical Properties[2]
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory
- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory
- Mathematical and Computational Sciences[2]
- Advanced Network Technologies
- Computer Security
- Information Access and User Interfaces
- High Performance Systems and Services
- Distributed Computing and Information Services
- Software Diagnostics and Conformance Testing
- Statistical Engineering

[1]At Boulder, CO 80303,
[2]Some elements at Boulder, CO.

NIST Special Publication 800-25

Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

Kathy Lyons-Burke

Federal Public Key Infrastructure Steering Committee

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2000

U.S. Department of Commerce
Norman Y. Mineta, Secretary

Technology Administration
Dr. Cheryl L. Shavers, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of Sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-25
Natl. Inst. Stand. Technol. Spec. Publ. 800-25, 33 pages (Oct 2000)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2000

For sale by the Superintendent of Documents. U.S. Government Printing Office. Washington. DC 20402-9325

Table of Contents

1. Purpose

This guidance document was developed by the Federal Public Key Infrastructure Steering Committee to assist Federal agencies that are considering the use of public key technology for digital signatures or authentication over open networks such as the Internet. This includes communications with other Federal or non-Federal entities, such as members of the public, private firms, citizen groups, and State and local Governments. Most public key technology applications for digital signatures provide for user authentication as well. However, public key technology can be used for user authentication only without digital signatures. Standards such as X.509 Version 3 (International Telecommunication Union Recommendation X.509 (03/00) - Information technology - Open systems interconnection - The directory: public-key and attribute certificate frameworks) provide for that functionality.

This document encourages the thoughtful use of public key technology by Federal agencies as set forth in guidance published by the Office of Management and Budget implementing the Government Paperwork Elimination Act (GPEA) (Public Law 105-277; Federal Register Notice, Volume 65, Number 85). GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with an agency the option to submit information or perform transactions with an agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal Government use of a range of electronic signature alternatives. This document also amplifies upon principles contained in the GPEA guidance and separately in *Access with Trust* issued in September 1998 by the Office of Management and Budget, the National Partnership for Reinventing Government, and the Government Information Technology Services Board. Finally, it discusses briefly the Government-wide Public Key Infrastructure (PKI) which is developing to enable applications programs to effectively use public key technology across Federal agencies.

Specific questions and issues are discussed to help agencies: (1) evaluate their potential applications of public key technology involving digital signatures or authentication, considering whether the application warrants such use as set forth in the OMB GPEA guidance; and (2) implement those applications selected. The questions and issues address technical, business, policy, and legal aspects, and they are fashioned to inform all agency elements who play a part in evaluating how public key technology may be applied to agency operations. While many of the factors addressed are also relevant to other (non-PKI) technologies used to support electronic transactions (e.g., Personal Identification Numbers), the focus of this document is the use of public key technology for digital signatures or authentication over open networks.

This document responds to the Office of Management and Budget (Federal Register Notice, Volume 65, Number 85) guidance on implementing the Government Paperwork Elimination Act. The guidance broadly addresses how agencies should assess the costs, benefits, and risks when moving to electronic processes. It also directs the Federal Public Key Infrastructure Steering Committee to publish technical guidance on the use of public key technology for

digital signatures or authentication. OMB has requested that other agencies issue related guidance on GPEA implementation. The Department of the Treasury is addressing policies and practices for electronic transactions and authentication techniques in Federal payments and collections; the Department of Justice is issuing guidance analyzing legal issues of electronic processes; and the National Archives and Records Administration (NARA) is providing guidelines on the management, preservation, and disposal of electronic Federal records when using electronic signatures. Readers are referred to those other documents for authoritative guidance on the issues they address.

2. Background

Individuals (including Federal employees) or other entities interacting with Federal agencies electronically where there is a need for a secure transaction should have reasonable assurance that:

(1) the information sender and recipient both will be identified uniquely so the parties know where the information is coming from and where it is going (identification and authentication);

(2) the transmitted information was not altered deliberately or inadvertently (data integrity);

(3) there is a way to establish that the sender's identity is inextricably bound to the information (technical non-repudiation); and

(4) The information will be protected from unauthorized access (confidentiality or privacy). This functionality is included for completeness since public key technology and a Public Key Infrastructure provide it; however, confidentiality and privacy concerns are not covered in detail in this guidance.

Two parties who may not know each other should be able to communicate reliably through electronic means, with confidence that their communication is protected and their identities are established with neither party being impersonated. They should also have assurance that their communication cannot be repudiated after it has occurred.

Public key technology enables applications software (programs) to meet these requirements. While a full description of the technology and how it works is beyond the scope of this document, a brief description can be found in *Access with Trust* and in a separate, more recent report, *The Evolving Federal Public Key Infrastructure* (both available at http://gits-sec.treas.gov).

Public key technology has a firm theoretical underpinning and a growing spectrum of applications, but its use represents unexplored territory for many Federal agencies. Natural reluctance may exist until the "bugs have been shaken out" by someone else. *Access with Trust* and *The Evolving Federal Public Key Infrastructure* describe how that "shaking out" process is well underway and succeeding in making public key technology in general, and

digital signatures in particular, useful to Federal agencies today. Federal agencies considering the use of public key technology will benefit by proceeding promptly to participate in building the Federal portion of the evolving worldwide PKI. This will enable agencies to develop applications around their needs, rather than adjusting those needs later to an evolving framework.

Decisions to apply PKI technology may be made for an agency if it postpones employing the technology in its applications software. Agencies may be forced to implement a specific PKI solution in order to interact with external entities that use a PKI. For example, the automobile industry, through the Automotive Network Exchange (ANX) and the International Computer Security Association (ICSA), is implementing a PKI for interactions with suppliers. In addition, the financial sector, through the National Automated Clearing House Association and through multi-bank consortia (one example is a multi-bank consortium under Identrus), is implementing PKI solutions for inter-bank interactions; and the health care sector, through hospitals, insurers, pharmacists, and others, is also implementing PKIs. The best way for Federal agencies to become full participants in the construction of the framework is to apply public key technology ***now*** to substantive agency work, just as companies in the industrial, financial, and health care sectors are doing for their spheres of interest.

As with any investment in new technology, the agency needs an appropriate business case linked to its mission and goals. An agency must ask itself whether the PKI functionality needs to be added for a specific Government function, whether it should be performed within the agency or through contractors or outsourcing, and whether the processes to execute the function need to be re-engineered. In many cases, the use of digital signatures may require transforming agency business processes to a new service delivery model, involving some degree of process re-engineering. In many instances, this can result in significant streamlining. Rarely can digital signatures simply be “plugged in” or “switched on.”

The public may have concerns about electronic transactions that PKI technology may not initially alleviate. People are naturally uncomfortable with change, and public key technology is not yet widely understood and it is not perceived as having demonstrated “trustworthiness.” To deal with these concerns, agencies should develop a public information plan or comparable document covering the agency's design, implementation, and presentation of the electronic application. The plan should seek stakeholder input early in the process of developing electronic transaction systems using public key technology, and it should establish and communicate the strengths which PKI technology brings to ensure security and privacy, promote the availability of electronic communications, and reduce risks associated with their use.

The Social Security Administration, which interacts with the public on a regular basis, published a report on this subject in September 1997 called “Privacy and Customer Service in the Electronic Age” (available online at http://www.ssa.gov). The report expands upon the issues discussed above and can help agency officials better understand how to deal with public concerns over electronic interactions.

As cited earlier, public key technology and digital certificates (which bind the identity of a party to his, her, or its public key) can be used to support authentication, encryption, non-repudiation, and data integrity. Several services are available through the use of a PKI, for example:

- A user can authenticate himself or herself to another party, typically a server, by digitally signing a challenge phrase (supplied by the server) with the user's private signature key. The server can use the public key in the user's digital certificate to validate the user's signature on the challenge phrase and thus authenticate the user.

- Web servers frequently have digital certificates issued to them which can be used to authenticate the server to a user and create an encrypted communications session that can be used to protect any shared secret information including Personal Identification Numbers (PINs) or passwords. Such an "encrypted session" can prevent a malefactor from taking it over (sometimes called "hijacking") after the session has begun.

- When web servers and clients both have digital certificates, mutual strong authentication can be achieved, and each party can authenticate itself to the other.

- A document or file may be digitally signed using a party's private signature key, creating a "digital signature" that is stored with the document. At a later date, anyone can validate the signature on the document using the public key from the digital certificate issued to the signer. Validating the digital signature not only confirms who signed it, but also ensures that there have been no alterations to the document since it was signed.

- Similarly, an e-mail message may be digitally signed using commonly available client software that implements an open standard for this purpose, such as Secure Multipurpose Internet Mail Extensions (S/MIME). Validating the signature on the e-mail can help the recipient know with confidence who sent it, and that it was not altered during transmission.

The X.509 Version 3 standard for digital certificates provides specific bits which can be set in a certificate to ensure that the certificate is only used for specific services (signature, authentication, encryption). Applications may or may not conform to the X.509 Version 3 standard and may or may not honor the bit settings in the certificate, so care should be taken to determine this prior to purchasing a specific product. Further, some communities of interest may set these bits differently while still complying with X.509 Version 3; thus, when different communities of interest desire to interoperate, they should establish how these bits are set to facilitate interoperability.

The guidance document is also intended to raise the awareness of agencies about uncertainties or concerns related to the use of public key technology. Thus a decision to use the technology, or how to implement it properly, can be fully informed.

Finally, this document focuses on the use of public key technology for digital signatures and authentication, but a PKI established for those purposes can also be used to provide end-user to end-user confidentiality or privacy through the use of encryption certificates. That is an example of the extensible nature of public key technology.

3. Access Certificates for Electronic Services

Agencies wishing to employ digital certificates should first consider using the capabilities provided by the Federal Technology Service (FTS) of the General Services Administration (GSA) through contracts under the Access Certificates for Electronic Services (ACES) program. ACES is a very convenient contract vehicle for:

(a) obtaining PKI services (including certificate issuance from a vendor PKI established especially for the purpose) for transactions with the public or with agency trading partners;
(b) obtaining vendor services to set up a vendor or agency-run special-purpose PKI covering agency employees, contractors, or the public; and
(c) obtaining vendor services to PKI-enable applications programs to accept certificates regardless of source.

In late 1999, the ACES program placed three contracts with large consortia, which included leading PKI and IT firms, and which provided competitive prices for digital certificate issuance and use. Agencies can make use of the ACES contracts simply by entering into an interagency agreement with FTS/GSA, and then let FTS manage the contract. Agencies are encouraged to consider this alternative as they review the guidance contained in this document. Agencies are encouraged to especially inquire as to the costs associated with enabling applications to use ACES, because the total costs associated with employing ACES falls well within the agency threshold for saving money through the use of electronic transactions requiring strong authentication. Further information and points of contact can be found at http://www.gsa.gov/aces.

4. Using This Document

Federal agency officials should determine if the use of public key technology for digital signatures and authentication makes good business sense. Agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. This determination often needs to be made on an application by application basis, with the understanding that once a PKI is in place, it can serve multiple applications. This document contains questions which Federal agency officials should answer while evaluating a potential application. The questions cover five main elements:

(1) the benefits derived from implementing and using digital signatures for an application;
(2) the costs;
(3) the risks;

(4) how to compare the benefits, costs, and risks to arrive at a decision; and
(5) what issues to consider in implementing the decision.

Associated with each question is additional material (labeled "discussion") to help provide a more complete context. There are questions about policy, technical, business, and legal issues, which address concerns of an agency's technical staff as well as its senior policy or decision-makers. Where this is likely to be the case and it is not clear from the context, the discussion material related to the question so indicates.

The questions (each of which starts on a new page) are presented in an order that anticipates how an agency may evaluate a potential application of public key technology involving digital signatures or authentication to an existing electronic process. Since one size cannot fit all, agencies certainly have the discretion to deal with the questions in a different order. Moreover, there may be circumstances where no electronic process currently exists but may be developed; in that case, the questions should be helpful in evaluating the potential application of this technology as the electronic process is designed. Finally, the questions help agencies compare PKI technology with other mechanisms such as PINs that supply some of the functionality provided by public key technology.

5. Summary

Many Federal agencies are implementing, or considering opportunities for implementing public key technology applications to improve the delivery of services both internally and to outside parties and to improve work processes with existing business partners. Recognizing these opportunities, and seizing them in a disciplined, thoughtful way, may involve accepting significant risks, as discussed in more detail below. Agencies should assess the risks carefully, seek to minimize them, and consider whether the risks they take are commensurate with their legal obligations and their duties to the public. Risks to be considered include those resulting from the use of digital signatures as well as the potentially higher risks resulting from continued use of other mechanisms such as paper based processes.

Fortunately, agencies wishing to seize such opportunities are not alone. They may call upon the experience and expertise represented by the many agencies that participate in the Federal PKI Steering Committee, the activities of which are reported in *Access with Trust* and *The Evolving Federal Public Key Infrastructure* and on the Steering Committee web site, http://gits-sec.treas.gov. Several of these agencies have already succeeded in applying the technology to a wide spectrum of applications. This guidance document aims to support agencies considering when and how to implement applications using public key technology for digital signatures and authentication.

Question 1. *What are the benefits, direct and indirect, financial and non-financial, objective and subjective, of using digital signatures for the proposed application?*

D1.0 Discussion

The context of this question includes converting existing electronic processes to use digital signatures; developing electronic processes using digital signatures where the existing process is manual; and considering external, inter- and intra-agency applications for the use of digital signatures. Further, as the question implies, benefits come in many forms. It is important for all of the benefits to be identified so that a fair comparison of costs and risks can be made. (For purposes of this discussion, "electronic processes" employ application software, so using digital signatures with an electronic process is tantamount to enabling the application software to accept such digital signatures. That, in turn, requires the application software to interact with the PKI under which the digital certificates are issued to end entities.)

Many of the benefits cited below accrue from the use of electronic processes, rather than from the use of digital signatures *per se* in those processes. However, as discussed above, public key technology can create a trusted environment that promotes the use and growth of *all* electronic processes, so it is appropriate to attribute these benefits in substantial measure to public key technology. Potential benefits that should be evaluated include:

D1.1 Time Savings

Use of electronic processes and digital signatures can reduce the time required to process information collections from sources inside or outside the agency. These may involve claims for financial or other benefits, bids on procurements, or simply inquiries involving private or proprietary information. Reduced response time benefits the agency by reducing per-transaction processing costs. The recipient benefits in ways that it may be difficult to measure, but which can be categorized as "increased responsiveness of Government to its citizens."

D1.2 Cost Savings

The long-term cost of performing agency business may be reduced. These cost reductions result from decreased transaction time and cost, increased accuracy and productivity, more effective use of staff in addressing agency priorities, reduced maintenance or operating costs associated with paper-based systems, and better and more trusted ways of allowing users to pay for services provided. These effects become more pronounced as the number of transactions increases.

D1.3 Enhanced Service

The availability and accessibility of agency processes to users inside the agency, to the public, and to other outside entities is enhanced. The strong authentication, which digital signatures provide, allows the agency to supply broader service and to promote Administration goals and objectives to a wider audience. With the burgeoning use of the Internet and the increasing sophistication of the American public in the use of electronic processes, microcomputers, and networks, electronic accessibility to Federal agencies provides an opportunity for a member of the public to contact a Government agency when and where it is convenient for the individual. In effect, Government can serve the public 24 hours a day, seven days a week. Many private companies are already operating in this fashion over the Internet.

D1.4 Improved Quality and Integrity of Data

With electronic processes using digital signatures, the quality and integrity of data collected are substantially improved. This reduces cost and improves process efficiency. For example, unlike paper processes, online forms can include field edit functions and immediate data integrity and consistency checks. Thus, errors can be detected during input and corrected at that time (i.e., before transmission), saving agency and customer time and effort. This approach also ensures the customer that the information he or she is providing will be accepted and that no errors were inadvertently introduced as a result of data-entry mistakes. These errors could be caused by poor penmanship on the part of the customer or by typographical errors on the part of the Government employee. Moreover, digital signatures provide strong authentication processes between the user and the system serving the user that help to assure users that it is safe to supply private information electronically and to receive the full benefit of electronic transactions.

These types of interactions are already becoming commonplace in the online market. Software providers encourage electronic registration of their products using query screens that prompt the user for information. The screens identify fields that must be filled out, provide options for entries, and generally check to ensure the fields contain legitimate information (e.g., checking that a phone number includes an area code; verifying that the zip code corresponds to the telephone area code; and so on). The organization and the user benefit when a single transaction with a customer requires only one interaction to satisfy that customer’s needs.

Question 2. *How much will it cost to (a) either convert an existing electronic processing system (that is, a system which processes information electronically or digitally) to use digital signatures, or convert an existing non-electronic process to an electronic one using digital signatures; and (b) operate such a system after conversion?*

D2.0 Discussion

Federal agencies perform this type of analysis whenever they consider implementing information technology in their work processes. Many of the requirements and considerations are discussed in OMB Circular A-130 and its references, or in requirements developed by each agency to implement A-130 and the Computer Security Act of 1987. This includes evaluating aspects such as the full life cycle cost of the system using digital signatures, system maintenance, facilities, training, backup, auditing, personnel needs, and other factors. Agencies should apply the same analytical methodology in evaluating the use of digital signatures for their electronic processes. The evaluation should touch upon the following issues in establishing expected costs:

D2.1 Required Level of Trust

The cost of implementing an application using digital signatures will depend on the level of trust (or assurance) that the application will be required to provide. Trust in this context means with what level of certainty the application meets the first three principles of identification and authentication, data integrity, and non-repudiation that are discussed in the Background section (2.0). The level of trust enables agencies to evaluate how well the system can defend against threats. The agency needs to establish how the required level of trust affects implementing digital signatures in the application (and attendant costs), and whether the technology should be used on a "per-transaction" or other basis. Agencies should consider:

(1) the nature of the transactions (e.g., number or frequency, and amount of information transferred per session), especially those containing information of programmatic or enforcement importance to the agency, financial information, or data requiring protection for privacy or proprietary reasons or otherwise particularly subject to the risks discussed in section D3;

(2) relevant statutory, regulatory, or other requirements, and trading partner practices;

(3) the level of assurance, if any, that the application currently possesses without digital signatures, measured against the principles of Section 2.0, and whether that level warrants changing;

(4) the scope of the application, especially whether it is anticipated to grow, because growth may create financial or other pressures that digital signatures can better address;

(5) the nature and expectations of the users, including their demographics and access to electronic methods of interaction; and

(6) the view of key stakeholders, such as privacy and consumer advocates.

D2.2 Integrity of Public and Private Keys

Public and private keys must be managed properly to ensure their integrity. The key owner is responsible for protecting private keys. The private signature key must be kept under the sole control of the owner to prevent its misuse. The integrity of the public key, by contrast, is established through a digital certificate issued by a Certification Authority (CA, discussed further below) that cryptographically *binds* the individual's identity to his or her public key. Binding the individual's identity to the public key corresponds to the protection afforded to an individual's private signature key.

Compromise or loss of a private signature key could have financial consequences if a user employing that signature key is conducting monetary transactions. A PKI includes the ability to recover from situations where an individual's private signature key is lost, stolen, compromised, or destroyed; this is done by revoking the digital certificate that contains the private signature key's corresponding public key (discussed further below). The user then creates or is issued a new public/private signature key pair, and receives a new digital certificate for the new public key. These activities incur transaction costs.

The Certification Authority (CA) plays a critical role in ensuring the integrity of public keys in the PKI. Upon being presented with proper evidence of identity (usually through a separate entity called a Registration Authority), the CA issues a digital certificate which contains the applicant's public key, identity, and other information (such as duration of the certificate), all signed by the CA's private signature key. The certificate may then be distributed or placed in publicly available databases, called repositories. The CA operates under a Certificate Policy (CP) and Certification Practices Statement (CPS) that collectively describe the CA's responsibilities and duties to its customers and trading partners. These policies include how the CA is conducting its affairs in compliance with its contracts and, where applicable, Federal or State laws. The uses for which a certificate may be employed depend upon the requirements surrounding its issuance; for example, the method of identity proofing by the RA before certificate issuance and how well the private signature key is protected.

The basic issues involving CAs that affect the cost of the application are:

(1) Whether the agency should operate its own Certification Authority; "outsource" that function, such as by employing a CA run by another Federal agency or one or more private companies (which may include the ACES contract offered by the General Services Administration to facilitate delivery of PKI services to agencies); or simply accept certificates signed by other Federal or commercial sector CAs.

(2) The level of "trust" the agency requires for the certificates to complete the transaction reliably. This includes determining the level of identity proofing required for a subscriber to get a certificate; the strength of the cryptography employed (e.g., key lengths and algorithms); how the corresponding private signature key is protected; and other factors. Agencies must determine the required level of trust premised upon several objective or subjective factors, including:

(a) Statutory requirements;

(b) Administration or agency policy;

(c) Trading partner practices.

(3) Will the CA need to interoperate with CAs run by other Federal agencies or with commercially available CAs, and if so, how that will be accomplished. Such interoperability is important if the agency wishes to have the certificates issued by its CA accepted by other parties, and if the agency wishes to accept certificates issued by other parties. Considerations include whether the agency CA will interoperate with the Federal Bridge CA (thus providing interoperability with all other agency CAs that interoperate with the Federal Bridge CA), and whether the agency CA will interoperate with other CAs via another mechanism.

(4) Will the CA need to operate 24X7; how often does certificate revocation information need to be published, including whether an online process needs to be in place for that purpose, such as using the Online Certificate Status Protocol; and is there a need for a local or remote backup CA to continue operation if the main CA goes down.

D2.3 Quantification of the Consequences of Potential Risks

The use of digital signatures entails potential risks, some of which are known and understood, others of which are known and less well understood (see *Question 3* below), and still others that may not yet be known. The consequences of each risk may be related in principle to a potential cost to the agency. For example, the agency may conclude that a higher incidence of fraud is likely. This may or may not be true

since many believe that the use of public key technology may actually reduce the incidence of fraud. Depending upon the particular situation and the way an agency implements its program, the agency may be able to define possible financial impacts by extrapolating losses due to fraud without digital signatures. To the extent that the consequences of a potential risk can be identified (per *Question 3*), an agency should consider whether its financial impacts can be quantified.

D2.4 Policy, Practices, and Procedures

Policies, practices, and procedures for the use of public key technology need to be developed for the application at issue. Indeed, the starting place on a policy level for a PKI is the development of a CP. If the agency has decided to run its own PKI, it should prepare a CPS. Writing these documents is likely to consume substantial resources, but those resources are well spent since they create the entire framework for the agency's PKI, including the issuance, revocation, and use of certificates.

Beyond the CP and CPS, existing agency policy, practices, and procedures may have to be altered or amended. Ideally, these processes should apply broadly to an agency's electronic transactions as a whole, or to classes of transactions, and there should be some consistency or common elements across the Federal Government.

The most important factors to consider in the development of a CP and/or CPS, and in any revisions to other agency policies, practices, or procedures, include:

(1) To what extent does the agency require a signature versus another form of identification for the internal and external process interactions in question;

(2) To what extent does the agency currently accept the use of digital or other electronic forms of signature for documents submitted within the agency, by other agencies, or by non-Federal Government parties including by the public;

(3) What auditing is required and what mechanism is employed to support the electronic and possibly encrypted nature of records;

(4) How the protection of personal information under the Privacy Act will be ensured. The use of public key technology may require the creation of new databases containing information that would make some of those databases "systems of records" under the Privacy Act. For example, when an agency either contracts for or operates its own Registration Authority, the database created for identity proofing purposes would be a system of records and thus would require notice in the Federal Register. Repositories of certificates maintained by an agency or by a contractor to the agency would also likely be systems of records. By contrast, however, a repository of certificates run by a commercial entity separate from the Government, for broader commercial purposes, but which the agency might access to obtain a person's digital

certificate, would *not* be a system of records. Questions concerning whether a new database required for the application of public key technology constitutes a system of records should be resolved with agency counsel and, if appropriate, the Office of Management and Budget.

(5) The length of time an agency must be able to present and/or validate a signature on a document. This affects:

(a) The duration for records retention for documents such as certificates and Certificate Revocation Lists (CRLs);

(b) The form of the electronic document, since once a digital signature is made, the document cannot be reformatted or otherwise changed without destroying the signature;

(c) What software and/or hardware may need to be retained in order to validate a signature made in the past;

(d) Requirements for trusted time-stamp services to determine the date/time of the signature, and of the documents (certificates, CRLs) needed to validate the signature in a trustworthy fashion; and

(e) Who should provide this capability? The ability to validate a signature on a document after the corresponding certificate has expired is an obligation that could be imposed on the component within the agency responsible for operating the CA, or on some central authority, which is responsible for the entire agency PKI. Further, agencies should consider how to ensure that the entity responsible for providing this service either will continue to exist or will have some mechanism providing for another party to assume its responsibilities in the event it ceases to exist.

(6) What the agency may want to require of subscribers (i.e., those to whom certificates are issued) prior to certificate issuance. For example, it is usually good practice to have a "subscriber agreement" in place that the subscriber manually signs. This agreement describes his or her obligations to protect the private signature key, and to notify appropriate authorities if it is stolen, lost, compromised, unaccounted for, or destroyed. Often the provisions of a subscriber agreement can be placed into other documents (such as an employment contract, or a security agreement). Agencies may also wish to consider periodic updating of user agreements, perhaps with wet signatures, as a security measure.

D2.5 Connectivity to Existing Agency Infrastructure

To use public key technology properly in an application, including establishing the PKI itself, proper connectivity must be provided to the agency's existing electronic infrastructure. This infrastructure may include extensive mainframe and other "back-end" information processing systems. Many of the infrastructure's systems employ security devices such as firewalls aimed at providing proper segregation and security. Virtually all devices have databases that may need to be used to support a PKI while maintaining their integrity. Thus, two issues warrant specific consideration:

(1) Identifying the parts of the existing agency electronic infrastructure that need to interface using public key technology and the parts to which an interface would be *desirable* but not essential is an important first step. The latter may include providing capabilities that are not critical to the specific application, but provide functionality desired by the agency for other reasons. Factors to consider include:

   (a) how the application and the PKI will function across security and access control devices such as firewalls;

   (b) how the application will interact securely with databases or directories that exist separate from the application but from which the application must obtain information (should those databases be replicated to minimize or reduce the need for such secure access.)

(2) Establishing the costs associated with providing the *necessary* and the *desired* interfaces, including those costs associated with making the transition to public key technology. For example, it may be necessary to operate multiple systems until the new one demonstrates reliable operation).

D2.6 Interoperability with Other Agency Infrastructures

Other connectivity issues which should be evaluated include appropriate connectivity to and consistency with (interoperability with) electronic infrastructures present in other agencies, and the Federal (and possibly non-Federal) PKI in general. Interoperability is a complex issue, which should be considered from several perspectives:

(1) Policy interoperability or how the "level of assurance" of certificates issued under the agency's Certificate Policy "map" to those of external parties. Doing such "policy mapping" depends upon several objective and subjective factors (e.g., comparison of identity proofing mechanisms; how private signature key protection is afforded; strength of cryptography; etc.). The Federal PKI Policy Authority performs this function for Federal agencies desiring to interoperate with the FBCA, so that the Certificate Policy of the FBCA becomes the "universal translator" of levels of assurance among agencies. In addition to policy mapping, another element of policy interoperability is ensuring that certificates conform to a consistent Certificate Profile, which describes the extension fields contained

within the certificates, how those fields are to be populated, and how they are to be interpreted by application software. The National Institute of Standards and Technology (NIST) has developed a Federal Certificate Profile that is useful for this purpose; it can be found by accessing the Technical Working Group web page through the Steering Committee web page (http://gits-sec.treas.gov).

(2) Technical interoperability comprises several elements:

(a) PKI to PKI interoperability. This is the ability of different CAs either to cross-certify or to accept some other mechanism (such as Certificate Trust Lists) so that the users in one PKI domain can accept as trusted (at some appropriate level of assurance) the certificates issued by another PKI domain;

(b) Application to application interoperability. This is the ability of different products to accept certificates issued outside their PKI domain, including the ability to create and process certificate trust paths from the domain of the relying party to the domain of the certificate issuer, using for example cross-certificates issued by the FBCA to both domains. It also means mapping policies using information in the FBCA cross-certificates to allow the relying party to establish how much confidence he or she should have in the certificate received from the sender's domain. Further, it means interpreting the extension fields in X.509 Version 3 certificates in a consistent and compatible fashion;

(c) Intra-application interoperability. This is the ability of different products to accept certificates issued by different CA products within their PKI domain. This can be vexing because CA products differ in the functionality they supply and the way they supply it. Each CA product generally needs to have an application "enabled" using a specific "toolkit" to accept its certificates. Once enabled, the application should work with certificates issued by that product. To have the application accept certificates issued by another CA requires the application to be enabled with yet another toolkit. While vendors are working to minimize this need to enable the application for multiple CA products, there will always be some elements that will require them. For example, each CA product does encryption key recovery differently, so it is not possible simply to "unplug" one CA product and "plug in" a new one seamlessly. The ability to do "plug and play" with many PKI products will improve with time, but it is unlikely that the interoperability problem will vanish;

(d) Directory interoperability. This is the ability to supply directory services that allow certificates and CRLs to be found and used to the PKI and applications.

In summary, an agency should determine what policy and technical interoperability is needed or may be needed with external parties, and then consider which products best fulfill those needs given the factors set forth above.

D2.7 Records Management

Proper management of electronic records maintained or used, as part of the application must be ensured. This entails:

(1) Retaining those records necessary for long-term system operation including, where appropriate, all certificates or CRLs produced by a CA;

(2) Retaining audit records and other materials necessary to establish proper system operation at any point in time as required for legal or other purposes;

(3) Ensuring past records stored using certain electronic formats or media remain recoverable as those formats or media are replaced with newer technology. For example, the use of 5 ¼ inch floppy disks is diminishing, and the number of microcomputer systems with 5 ¼ inch disk drives is also declining. This concern is not unique to public key technology, although the ability to preserve a digital signature does preclude the approach of simply reformatting documents, such as changing them from one word processor format to another word processor format. The digital signature is preserved when the file is transferred from one medium (e.g., magnetic disk) to another (e.g., optical media such as CD-ROM) as long as the transfer preserves the original file with 100 % fidelity.

For a thorough discussion of digital signature records management, the reader is referred to the guidance issued by NARA.

D2.8 Compliance with PKI Standards

There is no single Federal standard that defines and describes a PKI or the use of public key technology. There are, however, several standards (Federal Information Processing Standards (FIPS), American National Standards Institute (ANSI), and others) that are relevant to public key technology and a PKI. The standards, or a reference to a web site, from which they may be downloaded, can be obtained through the agency's Information Systems Security Officer or FPKI Steering Committee representative (URL http://gits-sec.treas.gov). Since some of these standards are in the process of revision to reflect the evolving nature of public key technology, it is important to contact the Steering Committee to ensure the agency's evaluation is based on the most recent information.

D2.9 Enabling Applications Programs

A PKI is an infrastructure, like a highway. By itself, it does little. It is useful when applications programs employ the certificates and services that it supplies. Applications programs either have to be PKI-enabled or PKI-aware out of the box (which is true of some applications such as secure messaging clients that employ S/MIME), or they have to be enabled separately. Such enabling may involve using PKI-vendor "plug-ins" which can be added into the application software, or it may involve far more detailed programming. Thus, agencies must understand the cost associated with making their existing applications PKI-enabled, and to ensure the ability to employ the PKI product or service selected by the agency for the infrastructure. With respect to interoperability, agencies need to understand that enabling an application to operate with one vendor's PKI products does not ensure that the application will also operate with a different vendor's PKI products. Indeed, at this stage, often the opposite is usually true. However, enabling a product to accept digital certificates issued to the X.509 Version 3 standard does afford interoperability. The application can accept such certificates from multiple vendor CAs, assuming that the certificates honor a consistent Certificate Profile for their extension fields.

D2.10 Apprising Affected Parties

Affected entities inside and outside the agency will need to be apprised of the availability of certificates and PKI-enabled applications. Subscribers to whom certificates were issued and users who may not hold certificates but may rely upon a certificate to decide whether or not to allow a transaction to be completed will need to be trained in their use. This includes processes from registration for certificates, to certificate issuance, to applications programs that rely on certificates for electronic transactions to be completed.

D2.11 Additional Statutory Requirements

In changing an existing electronic process to add in the use of public key technology, or in creating an electronic process using public key technology, agencies need to consider what additional statutory requirements they may need to meet. These include provisions of Section 508 of Public Law 105-220 governing providing Government services to individuals with disabilities.

Question 3. *What are the risks associated with the use of public key technology for this application?*

D3.0 Discussion

(1) Three areas of risks associated with the use of public key technology are (a) fraud; (b) failure of the system to fulfill its purpose (service failure or shortfall); and (c) liability. Agencies considering each area should evaluate risk in two separate contexts. First, does the use of public key technology create "new" risk? If so, what is its "absolute" level, that is, the greatest monetary or intangible loss the agency can suffer)? Second, how does that level of risk compare to the risk already experienced using existing systems that supply the same service to the public or other entities today? In other words, what is the relative risk?

The use of digital signatures may actually reduce risk compared to existing electronic and paper-based processes. Once a digital certificate has been properly issued, the ability to impersonate usually reduces to a simple question: can someone get that party's private signature key used for making his or her digital signature? If not, then identity fraud becomes extremely difficult. However, this raises an important issue for the Government: establishing the responsibilities and obligations of all parties in the new infrastructure, including those of individual users. Procedures must also be put in place to minimize the potential that a user could successfully repudiate his or her digital signature, for instance, by claiming that the confidentiality of the private key has been breached. Depending upon the perceived risk of fraud, this may require greater expense for initial identity proofing and to ensure proper protection and use of the private key.

There are reasons to believe that public key infrastructure-based systems have the potential for substantial public acceptance for transactions in the private sector. Even if the use of digital signatures exposes agencies' users to new fraud risks and creates increased uncertainty about prosecuting certain kinds of fraud owing to legal factors, such uncertainty may diminish with time as legislation is enacted or case law develops. The risks may be far outweighed by the economic and other advantages gained. For example, use of credit cards beginning in the 1950s significantly increased potential and actual fraud compared to the use of checks or other paper transactions for exchanging funds. Yet, as history has shown, the public has accepted that the benefits derived far outweigh the drawbacks. Likewise the potential for fraudulent use of cellular phones is far higher than for hard-wired phones in one's home, yet once again, the public has accepted that the benefits of cellular phone use far outweigh that drawback. Additionally, in both situations, industry has adapted and developed new controls and technology enhancements to reduce fraud while continuing to experience tremendous growth in these sectors.

Use of PKI technology by Government agencies is not entirely analogous to private-sector use. Government agencies may not be able to treat fraud as a cost of doing business in the way that businesses do, and the public may have different tolerance of risk in transactions involving Government programs than they do in transactions with private entities. Nonetheless, public use of digital signatures in their personal transactions is likely to enhance its acceptance for transactions with the Government. This acceptance can be further encouraged when agencies can demonstrate that they are taking all reasonable steps to ensure the use of this technology meets standards of care that are better than those practiced in the private sector. For a thorough discussion of legal risks, the reader is referred to the guidance issued by the Department of Justice.

D3.1 Fraud

Concerns have been expressed that the use of digital signatures in lieu of paper signatures will make it more difficult to prosecute individuals seeking to defraud the Government. Some people say that an individual who wishes to defraud an agency may submit a fraudulent claim for benefits, but that individual's signature on the paper embeds what are called "biometric" or "forensic" elements unique to the individual. In other words, his or her physical signature on the paper can be shown, by experts in court if necessary, to be bound to that person.

For digital signatures, however, there are no embedded "biometric" elements. The binding of the individual to the private/public key pair is done through the RA described previously using an identity proofing mechanism suitable for the ultimate intended use of the key pair. Thus, if a person "signs" a fraudulent claim with his or her private signature key (that is, he or she digitally signs the document), there are no physical or biometric characteristics which may be linked to that person by handwriting or other expert. Instead, with a PKI, the quality of the initial identify proofing and control of the private signature key used to sign documents become the critical factors, since the certificate issued by a CA relying upon the information supplied by a Registration Authority binds an individual to a public/private signature key pair.

For these reasons, Federal agencies planning to use public key technology for digital signatures must develop and make known obligations for managing private signature keys and establish appropriate policy governing their user and protection by subscribers. Subscribers must understand their obligations, and in some fashion (e.g., through a subscriber agreement), attest to that understanding, if they are to be held accountable in the event of a problem.

Additionally, applications which ask a subscriber to make a digital signature should be engineered so that: (a) the subscriber is clearly presented with an irrefutable description of what he or she is doing when asked to click on the button (and enter the authentication data to unlock his or her private signature key) resulting in the digital

signature being made; (b) there are appropriate statements attesting to the intent of the signer, and then captured on the document that is actually digitally signed; (c) the document that is actually signed is fully visible and "what you see is what you get" is honored; and (d) once the signature is made, and the document is sent to its destination, the destination replies with a "return receipt" that is also digitally signed by the recipient. These are considerations that strengthen the ability of the relying party to hold the signer accountable and make it more difficult for the signer to repudiate the transaction).

To provide additional signature strength, the relying party may require that signatures only be made using private signature keys created and stored on hardware tokens meeting appropriate FIPS requirements, and that applications programs (and the operating system on which they run) employ standards that make it more difficult for malicious code to be present or go unnoticed.

In summary, a robust digital signature implementation would ensure that: (1) the individual can be strongly linked to a particular transaction so that the signature captures the entire document, not just isolated elements such as the answers to questions held in a separate file; (2) it can be demonstrated that the individual intended to sign the document; (3) knowledge can be demonstrated that the individual knew exactly what he or she was doing when the digital signature was made); and (4) a digitally signed receipt is sent after the transaction, ideally reciting the relying party's view of exactly what was signed and the intent of the signature.

D3.2 Service Failure or Shortfall

An important goal of using electronic processes with public key technology is to ensure parties seeking Government services get those services quickly, efficiently, and with trust. But a service failure or shortfall having an adverse effect on an agency's ability to meet its legal obligations can result from factors such as poor design or implementation of the software providing or using the public key technology, or inadequate training of the service providers or users. Any process, electronic or paper, is susceptible to a range of risks, some of which are similar, others of which differ. Electronic processes may possess flaws in hardware or software that affect data integrity or availability, or impede data collection. Paper processes can be cumbersome, slow, and difficult to manage with respect to data security and availability. The important thing is that an agency does its best to identify the risks, both in new electronic processes and in extant paper processes. In this way, informed decisions can be made about making the transition from the latter to the former. The use of electronic processes in general, and those with public key technology in particular, creates risks that the system will not function as planned. At the same time, the level of service of paper-based systems is not high, and they too can fail to satisfy customers in quality or speed.

Agencies will need to develop methods to manage system failures or curtailments and deal with customer inquiries and complaints related to electronic transactions that use public key technology. Factors to consider here are the consequences to users of service delay or interruption; likelihood of delay or interruption; and ability to use a separate system until the electronic processes using public key technology are restored.

A related and equally important issue is the need to incorporate electronic services using digital signatures within the scope of agency disaster recovery plans. At a minimum, agencies should consider establishing backup sites for their key PKI components (RA, CA, directories) that supply the services necessary for applications programs to use certificates.

D3.3 Liability

Whenever a Federal agency interacts with outside parties, it must face the question of how its actions make it legally liable to affected parties. The use of public key technology is no different in this respect from the use of other technologies. This matter is addressed in the DOJ guidance cited earlier.

Question 4. *How should the benefits determined in response to Question 1 be compared to the costs established in response to Question 2 and the risks discussed in response to Question 3?*

D4.0 Discussion

This question involves a policy judgment, especially where the benefits contain both quantitative and non-quantitative elements. The agency must select the proper method to compare or weigh the costs against the benefits and come to an appropriate business decision about whether an electronic process using digital signatures is preferable to one that does not use that technology. An authoritative discussion of the costs, risks, and benefits of electronic processes appears in OMB's procedures and guidance on the implementation of GPEA (65 Fed. Reg. 25508 (May 2, 2000)). Some considerations that the agency should keep in mind as it performs this evaluation relative to the use of digital signatures are:

D4.1 Inherent Value

Ideally, the use of digital signatures should save the agency money in the short or long run. However, there are circumstances where the use of digital signatures may be warranted even without such savings. For example, building the good will of the public and elected State and local officials by demonstrating that Government services can be supplied more quickly and effectively in a trusted electronic environment may warrant substantial up-front and continuing costs. In that case, the issue boils down to whether there is sufficient value to the Government and citizens for the money being spent on the service, not just whether the service *per se* is saving the Government money. Agencies should consider whether an additional expense would be justified by increased or enhanced service.

D4.2 Part of a Bigger Whole

Agencies may find it useful to evaluate costs and benefits not simply on an application basis, but on an overall service delivery basis. The costs associated with establishing and running a PKI for digital signatures may support multiple applications and multiple agency programs, and therefore the same PKI over time will serve increasingly large numbers of customers and other capabilities such as encryption. Consequently, up-front development costs of the PKI may be evaluated as something to be incurred over time (like maintenance costs) and in the context of a total service delivery program.

D4.3 Public Acceptance

Even if the use of digital signatures exposes agencies to new fraud risks and creates increased uncertainty about prosecuting certain kinds of fraud as a result of legal

factors, such uncertainty may diminish with time as legislation is enacted or case law develops. The risks may be far outweighed by the economic and other advantages gained. For example, use of credit cards beginning in the 1950s significantly increased potential and actual fraud compared to the use of checks or other paper transactions for exchanging funds. Yet, as history has shown, the public has accepted that the benefits derived far outweigh the drawbacks. Likewise the potential for fraudulent use of cellular phones is far higher than for hard-wired phones in one's home, yet once again, the public has accepted that the benefits of cellular phone use far outweigh that drawback. Additionally, in both situations, industry has adapted and developed new controls and technology enhancements to reduce fraud while continuing to experience tremendous growth in these sectors.

D4.4 OMB A-130 Examination of Risk

The proposed application must meet the risk-based standard set forth in the Computer Security Act of 1987 and OMB Circular A-130, Appendix III, namely, is any benefit associated with the use of digital signatures for an application "commensurate with the risk and magnitude of the harm from the loss, misuse, or unauthorized access to or modification of the information?" This guidance provides substantial flexibility to agency managers. It recognizes that one size does not fit all, and that a sensible business application of digital signatures by an agency should recognize that agency's specific situation in managing data.

Question 5. *What are the critical implementation issues that an agency should consider as it seeks to implement and use a PKI for digital signatures?*

D5.0 Discussion

The introduction of public key technology requires considerable planning and may necessitate changes in business practices and service delivery models. Below is a checklist of the most important issues that agencies should consider in implementing and using a PKI for digital signatures. For each item, brief specific guidance is provided.

D5.1 ***Prepare a Certificate Policy and, if applicable, a Certification Practices Statement.*** These are the policy framework documents for the entire PKI, and they create the disciplined environment necessary for parties wishing to rely on certificates issued by the PKI. These documents in effect "map" the agency's business model for electronic transactions to the PKI, setting forth what types of certificates the agency will issue, purchase, or accept for its business needs. The CP should be prepared in PKIX Part 4 format (also known as "Chokani/Ford" framework), which lists all of the issues that the organization should consider. If the PKI serves multiple applications, and each application has a different entity responsible for it, then it is important to identify which organizational component has responsibility for developing and keeping up to date the CP and CPS so as to meet the needs of each application the PKI supports. The agency needs to create a CPS only if it is going to operate its own CA or have a contractor do it on behalf of the agency. Some CPS preparation may still be required if the agency obtains PKI services only; in that case, the agency will need to ensure that provisions of the CPS prepared by the service offerer are suitable for the agency's needs. Agencies should identify the critical employees who will actually run the PKI software, and be responsible for safeguarding and using the CA signing key.

D5.2 ***Decide what directory services are required by the applications that the PKI is intended to serve, and ensure they are available or are obtained.*** Such services allow the CA to publish CRLs so that users can readily discover them and allow users to easily obtain certificates for digital signature validation or encryption purposes. The certificates may not need to be obtained from this service if the certificates are conveyed as part of the transaction as with S/MIME clients.

D5.3 ***Ensure that the need for agency PKI interoperability with parties external to the agency is established and addressed.*** Use of the Federal Bridge CA will probably provide the most efficient mechanism to achieve interoperability with other Federal agencies. Agencies should consider the CP honored by the FBCA in preparing their Certificate Policies.

D5.4 ***Ensure that as the PKI is developed, agency applications are made PKI-enabled (or purchased PKI-enabled).*** Application programs that use the PKI should

be planned concurrent with the selection and implementation of the PKI. This procedure provides the greatest flexibility since both the infrastructure and the applications programs can be adjusted to fit. This effort includes ensuring that applications programs can create appropriate certificate trust paths; process those paths; and find and check certificate revocation information through Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), or validation authorities. Moreover, this is the time to ensure that the applications contain the proper user "interface." They should fulfill the legal requirements to minimize risk and provide information suitable for later litigation, such as appropriate jurats, notices to users about the meaning of their making a digital signature, and so on.

D5.5 ***If practical, implement the PKI and applications in stages rather than all at once.*** Incremental implementation provides maximum opportunity to "learn as you go" and make adjustments as the process proceeds. Moreover, it allows the agency to scale up such functions as a "help desk" as the number of users increases, rather than having to start with a large help desk, which can be manpower intensive.

D5.6 ***Where practical, integrate PKI registration processes into established personnel or security practices.*** Agencies can allow employees to register to obtain a digital certificate when they obtain an agency identification credential, are certified or qualified to perform a function, or get a security clearance. This approach also has the advantage of allowing an agency to place into standard employment or security paperwork the subscriber agreement, which an employee must sign as a condition of getting the digital certificate. It also supports periodic updates to the agreement if that is determined to be necessary. Finally, this approach is consistent with the points in D5.5 concerning incremental ramp-up.

D5.7 ***Identify (and act upon) requirements to make the PKI software, directories, and applications programs operate through firewalls and routers***. For example, many PKI programs require certain TCP/IP ports be available (open). Executing PKI services through firewalls may require obtaining approval of system security personnel.

D5.8 ***Decide whether to employ CRLs, OCSP, or a "Validation Authority" approach for publishing or making available certificate revocation information.*** The CRL approach is employed by most commercially available software today; the OCSP approach is analogous to the current credit card model that is used extensively; the validation authority approach, for which there are also commercial products available today, involves establishing a central location into which certificate revocation information is published from multiple CAs to facilitate certificate status checking. In establishing conditions that require certificate revocation, agencies should determine and balance the trade-off between a stringent policy that results in a large number of revocations, and a less stringent policy that results in fewer revocations. Greater number of revocations can have an adverse impact on the

performance of the PKI, especially if CRLs are used as the mechanism for conveying information on certificate status to applications.

D5.9 ***Decide whether to employ an online (e.g., HTTP-based) or off-line (e.g., S/MIME) functionality — or both.*** S/MIME (Secure MIME) is an open standard for messaging (e-mail) which includes digital signatures on documents and messages, but it does not provide for an interactive environment. By contrast, browser-based models support interaction but do not yet have open standards reflecting how HTML or XML pages are digitally signed. All such solutions currently available employ proprietary approaches and thus may not be interoperable between products. Efforts are underway to establish an open standard for XML digital signatures, but how quickly that will be completed is uncertain.

D5.10 ***Establish who will fulfill audit roles for the PKI.*** These roles may reside within the office of the agency's Chief Information Officer; within the Inspector General's office; within the office responsible for information security; or somewhere else.

D5.11 ***Address any liability issues that warrant consideration.*** This includes stating what liability, if any, the agency is able and willing to incur in the use of certificates it issues, and if so, under what circumstances. Generally speaking, the agency PKI should be viewed as another way to convey or preserve trust between transacting parties (established pursuant to other relationships such as contracts or regulations), rather than creating trust per se.

D5.12 ***Resolve how to deal with validating a digital signature well after it is made.*** All of the information required to validate a digital signature after the relevant certificates have expired should be available. This includes the expired certificates and the CRLs or other information showing that the certificates were valid at the time the signature putatively was made. It also includes deciding who is responsible for providing long-term signature validation services. That is, should the organization responsible for relying on that signature be able to perform the validation, or should the infrastructure provide that capability "automatically"? Answering these questions requires understanding about how long the agency wishes to be able to validate a signature, and whether it is willing to accept something other than original signature validation. For example, the agency could decide to accept the validation of a signature made by a digital archivist that the signature was validated as of some date subsequent to its having been made. Indeed, as the cryptographic strength of a digital signature diminishes with time, it may be necessary to have a trusted party (sometimes called a "digital archivist") oversign the original document (and original signature) periodically, using a signature with stronger cryptography.

Appendix (1): Description of Public Key Technology and the Public Key Infrastructure

A1.0 Public key technology and a PKI depend upon complicated mathematical concepts, but their effects are simple and understandable. When a Federal agency (or employees of such an agency) starts to use the PKI, the agency (or an employee of that agency — call that person "Bob") begins with a pair of "keys," which look like very long character strings and are actually digital representations of very large numbers. These keys are either generated by Bob using a local cryptographic module or provided through trustworthy mechanisms, subject to certain mathematical requirements. One of these keys is secret (*private*) and the other is published (*public*).

A1.1 The essence of public key technology is that messages or transactions authenticated or encrypted using one of Bob's keys can only be verified or decrypted using his other key. Thus, when Bob uses his private signature key to sign an electronic message or other transaction digitally, anyone who knows Bob's corresponding public key can verify Bob's signature. A similar method using public key technology can be used to encrypt messages for confidentiality as they transit an open network such as the Internet.

A1.2 The PKI uses special digitally signed messages (called "certificates") to bind Bob's identity to his public keys. A digital certificate is issued by a trusted "Certification Authority" (CA) and signed using that CA's private signature key. When someone else (call her "Alice" — she may be a private citizen, a company, a public interest group, or some other entity seeking to interact with a Federal agency, or she may even be an employee of that Federal agency or a different agency) wants to obtain with certainty Bob's public key, she gets Bob's certificate. Where or how Alice gets Bob's certificate is not important - she may get it from Bob in person, or from an online "repository" for certificates, or from Bob's homepage on the World Wide Web, or from Bob's credit card issuer; once she gets it from whatever source, Alice checks the certificate by validating the CA's digital signature. Alice now knows Bob's public key and name with certainty and can validate any messages sent to her, which were signed with Bob's private signature key. These transactions may be conducted with assurance even though Bob and Alice may have never met; and although they sound complex, they can be done automatically by the underlying network of computers with no burden placed on Alice or Bob.

A1.3 To validate the CA's signature on Bob's certificate, Alice must first know the public key of Bob's CA. Alice always knows the public key of at least one CA that she trusts. CAs may issue certificates to each other. If Alice does not know the public key of Bob's CA, she may still be able to find a certificate issued by a CA whose key she does know, that certifies the public key of Bob's CA. In essence, a CA Alice trusts "vouches" for one she does not know. Much of the challenge of building a robust global PKI is in the management of certificates between CAs, as well as the software and infrastructure that automate the process of building and validating these trust chains of certificates.

A1.4 As a general matter, good security practices will ensure Bob has different public-private key pairs for signature and confidentiality uses, and to reflect his different roles (e.g., as an agency official, and as a private citizen and consumer). This is analogous to a person having different passwords for use on different computer systems, or different Personal Identification Numbers (PINs) for use with different financial accounts.

A1.5 The scientific, academic, and business communities recognize that the capabilities described above provide the best way to replace handwritten signatures in the electronic world, to authenticate identities securely, and to maintain confidentiality on open networks. Realizing this vision of transacting electronic business with security and privacy requires that the various implementations of public key technologies work together smoothly and in a fashion transparent to the user — which is one of the goals of this document.

A1.6 Finally, it is useful to describe briefly the PKI itself. The PKI is not simply software or hardware. It is an *infrastructure*, that is, a combination of products, services, facilities, policies, procedures, agreements, and people that provide for and sustain secure interactions on open networks such as the Internet. It is not a single monolithic entity, but a distributed system in which the component elements may include public key infrastructures that are interoperable and interconnected. The infrastructure provides assurances that information is protected while being entered, during transit, and when stored. The underlying technology is already developed by private industry and is being marketed and used commercially. The PKI promotes interoperability among commercial products and the early integration of security features into those products.

A1.7 The PKI can be likened to elements of the telephone network. When one wants to contact someone else, it is necessary to access a phone directory or an information operator to get that person's telephone number — analogous to the role that a directory (run by the CA or some other entity) plays in supplying a digital certificate of the person to be contacted. When someone moves to a new location and changes telephone numbers, the infrastructure must adjust its information to reflect that fact. When you want to know the number of the person who has dialed you, "caller-id" provides that — another part of the telephone network infrastructure analogous to the authentication process in public key technology.

A1.8 Finally, for a complete description of public key technology and its relationship to electronic transactions, two useful references are *Secure Electronic Commerce* by Ford/Baum, and *Applied Cryptography* by Schneier.

Appendix (2): Description of Public Key Certificates and the Certification Process

A2.0 The PKI employs a Certification Authority (CA) to provide digital certificates binding the identity of an individual to his or her public keys. (An individual may have more than one public key — for example, for acting as an agency official or as a private citizen — but a digital certificate includes a single public key.) A separate entity, called a "Registration Authority" (RA), may be used to certify the individual's identity to the CA so that the CA will issue a digital certificate.

Thus, for a user (who is known as a "subscriber" in this context), the process of getting a digital certificate for the first time may entail:

> Step 1: Generating (or having someone generate for the user) a key pair containing a public and private component; if someone other than the user generates the key pair, then the subscriber incurs some risk of misuse since his or her "private" key is known by at least one other entity;
>
> Step 2: Going to the RA (which may or may not be part of the CA) with proof of identity and a copy of the public key; in some cases, where the required level of "identity-proofing" is not high, it may be possible to do this online with appropriate safeguards such as those envisioned in the GSA Access Certificates for Electronic Services (ACES) effort;
>
> Step 3: At the RA, physically signing some paperwork (so that a physical signature is on file), which accepts for the subscriber the responsibility for the protection of the private signature key (corresponding to the public key) and its use.

A2.1 After following its procedures to verify the identity of the individual requesting a digital certificate, the RA communicates electronically with the CA who issues the digital certificate (signed with the CA's private signature key) binding the subscriber's public key to his or her identity. The CA then usually places the certificate in a public database, called a repository, which may hold certificates issued by many CAs. Repositories can be replicated, be online, and be freely accessible, with much less protection than CAs require.

A2.2 When a user (Alice) needs to communicate with another user (Bob), Alice obtains Bob's certificate containing his public key from a repository. Bob's certificate is signed using the private signature key of the CA. Alice then verifies the CA's signature on Bob's digital certificate using the CA's public key, and recovers Bob's public key. These functions are normally done automatically by the software in a fashion transparent to the user. Note that if someone from outside this process were successful in surreptitiously substituting into a repository's data base a bogus certificate for Bob with a different public key, the signature on the bogus certificate would not validate with the CA's public key because it was not signed

by the CA's private signature key. This is an example of the safeguards embedded within public key technology. It does not matter where or how Alice gets Bob's certificate (Bob could even physically hand it to her on a disk), since it is the CA's signature on the certificate which authenticates it.