The Evolving Federal Public Key Infrastructure

Federal Public Key Infrastructure Steering Committee

Federal Chief Information Officers Council

This document is available electronically at gits-sec.treas.gov

The Evolving Federal Public Key Infrastructure

Table of Contents

Executive Summary

Introduction 1

The Elements of Public Key Technology 2

Technology Implementation Issues 5

The Role of the Private Key 5
The Role of Standards 6
The Recovery of Encrypted Data 7

Environment and Oversight 7

The Statutory Landscape 7
The Federal PKI Landscape 9
Access Certificates for Electronic Services 10
Governance of the Federal PKI 11
Interoperability of the Federal PKI 13
The FBCA Prototype and Electronic Messaging Association Challenge 2000 15
Public Key Technology and Critical Infrastructure Protection 16

The Future 17

Credits 18

Appendices 19

Executive Summary

Impelled by statutes, administrative policies, and the recognition that electronic transactions promise to provide far greater efficiencies and improve service delivery to the public and trading partners, Federal agencies are using the Internet for an increasing spectrum of applications. Doing so requires that agencies confront the issues of user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary.

While there are many technologies which meet some of these requirements, only one provides the tools for meeting all of them: public key technology, implemented in the form of a Public Key Infrastructure (PKI). As agencies implement PKIs suited to their needs, they are discovering that one of those needs is the ability to interoperate with other Federal and non-Federal agencies; that is, the ability to have electronic credentials (called digital certificates) which an agency issues to its employees or trading partners accepted by other agencies. This recognition has prompted extensive discussion of the mechanisms available for interoperation, and the development of one in particular, called the Federal Bridge Certification Authority, which promises to provide peer to peer interoperability that honors the autonomy agencies enjoy pursuant to statute and practice.

This report discusses the full spectrum of Federal PKI activities, from efforts by individual agencies to develop and deploy their own PKIs, to efforts by the General Services Administration and others to support interoperability of those PKIs and provide services aimed at promoting a single infrastructure for interactions with the public. The report tells the story of substantial growth in the use of PKI by the Federal government, because of the growing maturity of PKI products and increased understanding of just how flexible the technology is – a single infrastructure supplying a spectrum of interoperable services that can meet a variety of agency security needs.

Richard A. Guida

Richard A. Guida

Chair, Federal PKI Steering Committee
June 2000

Introduction

In 1997, Vice President Al Gore published *Access America*, a report which outlined actions the Federal government is taking to promote the electronic delivery of services, and electronic transactions between agencies and trading partners, over open networks such as the Internet. The report made it clear that providing a proper security infrastructure was essential for electronic transactions to flourish.

In 1998, the Office of Management and Budget (OMB) and the Federal PKI Steering Committee, in conjunction with the National Partnership for Reinventing Government, published *Access with Trust*, a report describing Federal agency efforts to employ a specific security technology – public key cryptography – which is particularly well suited for achieving authentication, information integrity, non-repudiation, and confidentiality of transactions over open networks. *Access with Trust* described agency pilot efforts using public key technology, and it set forth certain principles which would guide Federal adoption of this technology: (a) the use of commercial off-the-shelf software to the maximum extent practical; (b) the use of open vice proprietary standards; (c) a strong bias towards product neutrality – that is, allowing agencies to select whatever products they determine will best suit their needs; and (d) a strong desire to deploy solutions which are interoperable, scalable (having the ability to serve large numbers of users), and extensible (having the ability to serve multiple applications from one infrastructure).

This report builds upon the previous two. It provides an updated picture of how public key technology is being used within Federal agencies, describing a burgeoning expansion as planned and predicted in the previous documents. Further, this report lays out a strategic vision for the continued evolution and development of the Federal Public Key Infrastructure (PKI), focused on promoting continued expansion within Federal agencies, interoperability among Federal agencies (and ultimately interoperability with the private sector), and the development of appropriate mechanisms for governance that support innovation and growth.

The Elements of Public Key Technology

Public key technology provides a mechanism to authenticate users strongly over closed or open networks, ensure the integrity of data transmitted over those networks, achieve technical non-repudiation for transactions, and allow strong encryption of information for privacy/confidentiality or security purposes. Strongly authenticating users is a critical element in securing any infrastructure; if you cannot be certain with whom you are dealing, there is substantial potential for mischief. Ensuring the integrity of data from end-user to end-user makes it more difficult for data substitution attacks aimed at servers or hosts to succeed. Technical non-repudiation binds a user to a transaction in a fashion that provides important forensic evidence in the event of a later problem. Encryption protects private information from being divulged even over open networks.

Public key technology differs from systems using "shared secrets" or symmetric cryptography. In the latter, users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server, or between two or more users. A single key, again shared between two parties, provides communications privacy. The sender (to encrypt a transmission) and the recipient (to decrypt that transmission) use the shared key in an algorithm (agreed too beforehand by the transacting parties).

Symmetric cryptography has several inherent limitations that become acute when the transacting parties have no prior relationship. First, each pair of transacting party's needs a unique shared secret key – or else impersonation or eavesdropping becomes a problem. This means that the approach does not scale well – each user must have as many keys as people with whom he or she must deal. Second, once one party generates a secret key, that key must be transported securely to the trading partner, which can cause immense logistics problems and delays. Finally, because the individual must share the key with a trading partner, non-repudiation is lost. What this all means is that symmetric cryptography, by itself, is not conducive to e-commerce or e-government.

The limitations of symmetric cryptography are overcome using public key technology, which is also called "asymmetric cryptography." In a typical Public Key Infrastructure (PKI), two key-pairs are generated by or for each user, one key-pair for digital signatures and authentication, and the other key-pair for encryption. Each key-pair comprises two keys (very large numbers, typically 150 to 300 digits in length) which are mathematically linked in a very subtle way. For each key-pair, one key is kept private, and the other is made public.

Each public key is made public in the form of a digital certificate where a trusted party (called a Certification Authority or "CA", which may be within or external to the agency) cryptographically binds the public key to the person's identity by digitally signing the certificate. The digital signature on the certificate ensures that any unauthorized alteration of either the identity or the public key will be detected.

The mathematical algorithm used for generating the keys, and the size (length) of the keys, can be selected to provide virtually complete assurance that the private key cannot be deduced from the public one. In the case of a commonly used algorithm called "RSA," this can be done because information available at the time of key pair generation (where the private key *is* deduced from the public one) is immediately discarded and cannot be recreated.

Because public key technology uses two keys, one of which is kept secret and the other made public, there is no "shared secret" between the transacting parties, and thus no opportunity for one party to compromise the interests of both by losing control over the "shared secret." There is also no need to manage large numbers of symmetric keys (since each set of transacting parties would need a unique symmetric key). The user makes the digital certificate available to whomever he or she wishes to conduct business with.

As long as the user keeps his or her private key private, a malefactor will have great difficulty attempting to impersonate the user or obtain private communications simply by attacking the remote computer or server – because there are no "shared secrets" used for these purposes. This is a critical point, because many attacks focus on large data bases of shared secrets – passwords, PINs, and the like – held at hosts or servers which, by their nature, must be available for access by multiple users and applications in order to provide the functionality for which they were designed. If the data base can be successfully compromised using dictionary or other attacks which rely upon finding one or a few commonly used passwords from a long list (even where the passwords are encrypted), a user's account or interests can be compromised without the user's knowledge and even if the user did nothing wrong. With public key technology, the user normally must do something wrong to be at risk: he or she must compromise the private key in some fashion.

In a common form of digital signature associated with e-mail, when the user wishes to sign a document digitally, he or she applies the private signing key to a hash of the document being signed which transforms the hash into a new, different value. The hash is like a unique fingerprint of the document, expressed in the form of a large number. The user then sends

To describe an analogous situation using fingerprints, consider a case where the message sender wishes to send an emissary whom the recipient can trust. The sender takes the emissary's fingerprints (the "hash"), then seals the fingerprints in an envelope on which the sender signs his or her name manually so that it would be apparent if the envelope had been opened by anyone else (the envelope and content now constitute the "signed hash"). The emissary then carries the envelope and presents himself or herself to the recipient. The recipient takes the fingerprints of the emissary as he or she arrived; takes the envelope, verifies the written signature on it (converts the "signed hash" to the original hash), then opens the envelope and compares the fingerprints inside the envelope to those just taken from the emissary. If they are identical, the emissary is deemed to be the person sent by the sender. While this analogy is not perfect, it illustrates the concept in a human setting.

The action of digitally signing and then validating the signature to authenticate the sender provides data integrity for the document because any change to the document after the original hash is generated and signed would cause the signature to fail to validate. This affords *technical* non-repudiation – the user cannot later deny that his or her private signing key was used to make the digital signature. Of course, it is still necessary to demonstrate that the user had control of the private signing key to establish *legal* non-repudiation.

A sender can encrypt a document so that only the intended recipient can decrypt it. To do this, the sender generates a one-time symmetric encryption key (called a "session key") and uses that to encrypt the document. The sender then takes the public key of the recipient, encrypts the symmetric session key with that public key, and sends the encrypted session key plus the encrypted document to the recipient. The recipient, in turn, applies his or her private key to decrypt the symmetric session key, then uses that to decrypt the document. This combination of symmetric and asymmetric cryptography is done for reasons of computational efficiency, since the former can be done much faster on a computer than the latter. This is especially important for large files. Again, the e-mail software performs these functions automatically – the user does not have to go through each step manually.

Good security practice requires that the key-pair used for encryption should be different from the key-pair used for digital signatures. Why is this necessary? Because it is wise to have a copy of the private key used for decrypting information in the event the original copy is destroyed (otherwise there is no way to decrypt information encrypted using the corresponding public key). However, a copy should never be made of the private key

used to make digital signatures. Thus, two key-pairs are needed. This point is discussed further below.

Technology Implementation Issues

The Role of the Private Key

For most implementations, the private key is held on a hard disk and "unlocked" (i.e., made available to sign or decrypt information) with a PIN or password that is a "shared secret" between the user and his or her computer. For added security, the user may create and hold the private signing key on a hardware token such as a smartcard, and then use a PIN, password, or biometrics identifier (like a fingerprint) to unlock that key for use. To emphasize, the PIN, password or biometrics identifier in this case is a shared secret between the user and his or her smartcard – not between the user and a remote host or server, and not even between the user and his or her computer. Thus, as long as the user retains control of the smartcard, the system remains secure. If a biometric identifier is used to unlock the private key for use, then security is further enhanced because the malefactor must get the smartcard and a copy (somehow) of the biometric identifier.

Smartcards, which provide for key pair generation on the card, may also provide for signing events to occur on the card. In other words, the hash of the document to be signed is provided to the card by the application program, and a microprocessor on the card executes the signing event and returns the signed hash to the application program. This approach provides the highest security – the private signing key is generated on the card and never leaves it even for signing events.

Some smartcards possess vulnerabilities that may allow a malefactor to deduce their operations by measuring power consumption or the timing of certain events. These types of attacks, however, usually require physical possession of the smartcard (or insertion of the smartcard into a reader which has been maliciously altered in some fashion), sophisticated laboratory equipment, and exquisite knowledge of smartcard operation, so they are not usable by a remote hacker or by a common thief who may steal the smartcard. Further, newer smartcards employ power spectral filtering or other technologies that make them less susceptible to these attacks.

While the value of public key technology is most evident for transactions over open networks, where user authentication can be particularly vexing, the technology is also valuable in closed networks. It not only affords strong

authentication; it also provides a means to track what authorized users are doing. This does not raise privacy concerns since actions taken within the scope of one's employment using government equipment are always subject to review and scrutiny. After a user has been authenticated, the operating system or application software may require that transactions be digitally signed, thus resulting in a unique user identifier being placed on each transaction. This provides traceability, makes it difficult to perform tasks anonymously or under the guise of a different user, and in doing so, mitigates the "insider" threat.

The Role of Standards

There is a wide spectrum of standards applying to public key technology and products. The standards range from those focused on functionality, to those whose goal it is to promote interoperability, to those intended to support security. Most of the standards originate in the commercial sector, from the Internet Engineering Task Force or from contractors who supply PKI products or services. Within the Federal government, two agencies – the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) – are the principal sources of standards and requirements used by Federal agencies on this subject. A list and descriptions of relevant Federal standards can be found through the NIST web site at http://www.nist.gov.

Related to standards is the issue of accreditation, or measuring compliance with the standard. For example, under the NIST Federal Information Processing Standard for Cryptographic Modules (FIPS 140-1), vendors who assert that they comply with the standard go through a formal certification process at a NIST-approved private laboratory, and then are issued a document attesting to their product's conformance to the standard. Federal agencies are required to use products that are so certified unless a waiver is authorized.

NIST and NSA will continue to publish new standards and requirements to help ensure the technical integrity of PKI products. Some of these requirements will stem from the Common Criteria published under the International Standards Organization, and will include certification of products under protection profiles established based on application needs, or security targets based on the capabilities of vendor products. This approach will help to harmonize on an international level the way in which PKI products can be judged.

The Recovery of Encrypted Data

Whenever data are encrypted using someone's public key, there is always a risk that the corresponding private key could be lost or corrupted, making it impossible to decrypt the information. Because of this, and for reasons of business continuity alone, agencies understand that it is important to have the ability to recover encrypted stored data. That is, they must be able to decrypt information even if the individual who has the necessary private key can't find or use it for that purpose. This is analogous to maintaining a copy of the combination to a safe separate from the person who uses the safe. There are several ways to effect data recovery, ranging from making a separate copy of the private decryption key and placing it under the control of appropriate agency authorities, to saving the session key (that was used to encrypt the data) in some other form suitable for decryption by other than the recipient (this is sometimes referred to as "session key encapsulation"). But two elements are paramount: (a) the inescapable need for an agency to be able to recover encrypted data; and (b) the fact that fulfilling that need must not result in any copies being made of private keys used for digital signatures. This latter element requires individuals doing both digital signature and encryption activities to have two separate key pairs (and two certificates), one for each purpose.

Environment and Oversight

The Statutory Landscape

Business-to-business and business-to-consumer electronic commerce has burgeoned over the past several years, the former reaching $43 billion and the latter $8 billion in 1998. Estimates predict that by 2003, those totals will exceed $108 billion and $1.3 trillion respectively (Forrester Research). This experience suggests that electronic forms of authentication which are accepted over the Internet – and which include the use of public key technology – are generally accepted as having sufficient legal foundation by the transacting parties to allow e-commerce to proceed and grow.

Nonetheless, state legislatures are enacting laws dealing with electronic signatures to provide a uniform framework and thus promote acceptance of electronic signatures across state boundaries. For example, the National Conference of Commissioners of Uniform State Laws is working on changes to the Uniform Commercial Code, intended to regularize digital signature

practices nation-wide. These provisions would then be adopted in model state laws.

At the Federal level, in October 1998, Congress enacted the Government Paperwork Elimination Act (GPEA, Public Law 105-277) requiring that when practicable, Federal agencies by October 2003 accept forms electronically with electronic signatures. Electronic signatures are a superset of digital signatures. Subsequent Administration directives, including memoranda from the President to executive agencies in December 1999 have reinforced this theme. GPEA also provided that electronic signatures used in transactions within or with the Federal government shall not be denied legal effect or validity simply because they are in electronic form.

Under GPEA, OMB was tasked to produce implementing guidance which covered, among other things, the use of electronic signatures to facilitate adoption within Federal agencies. In March 1999, OMB published draft guidance for public comment (Federal Register March 99: Volume 64, Number 43, Page 10895). The draft guidance discussed the spectrum of different electronic signature mechanisms – PINs, passwords, biometrics, digitized signatures, and digital signatures – and advised agencies that the technology selected needed to be suited to the level of authentication required by the application. After careful consideration of comments received on the draft guidance, OMB issued final guidance (Federal Register May 2000: Volume 65, Number 85, Page 25508).

Although the deadline for implementing agency electronic service delivery initiatives is over three years away, GPEA is impelling agencies now to consider electronic signature alternatives for their applications. In particular, the final OMB guidance calls for agencies to submit to OMB by October 2000 their plans to comply with GPEA. The OMB guidance recognizes that digital signatures provide a particularly robust means for authenticating individuals, and doing so in an interoperable fashion – that is, one electronic credential (a digital certificate) can readily serve multiple applications across multiple applications. Because of these considerations, many agencies are predisposed towards using public key technology as a solution. OMB's 1999 annual information resources management bulletin included a data call asking agencies to outline their present electronic service delivery initiatives, and to summarize their plans to meet the October 2003 target. Agency responses are being compiled by OMB; they will be made available in a separate report.

The Federal PKI Landscape

Within the Federal government, substantial efforts are already underway to deploy public key technology for intra-agency applications, especially those involving personnel matters, contracts, and financial transfers. These efforts include implementing agency public key infrastructures providing the full range of services needed to issue and manage digital certificates: Registration Authorities (called "RAs") to identity-proof users, Certification Authorities (CAs) to issue certificates, repositories to manage certificate revocation lists, directories to hold certificates, and key recovery agents to allow the recovery of encrypted data if the private decryption key is lost. A wide range of PKI products and services exists supporting such enterprise-wide needs. As yet, these products do not universally support interoperability if different brands are employed between enterprises. Since the Federal PKI is developing from the bottom up, with agencies picking disparate products and services suited to their needs, a complex environment is emerging in which to effect interagency interoperability. Steps to deal with this environment are described below.

With respect to their use of public key technology, Federal agencies generally can be placed into one of three groups. The first group comprises early adopters, those agencies that have performed pilot PKI efforts and are migrating towards production use of the technology. The second group comprises agencies that are planning or executing pilot efforts preparatory to ultimate production use. The final group comprises agencies that are considering public key technology for future use but that do not yet have specific plans for pilot or other efforts. These different groups constitute a spectrum, a phenomenon that is to be expected in the adoption of any new technology. The spectrum is shifting strongly towards the use of public key technology.

Appendix A to this report describes the efforts of Federal agencies employing public key technology for authentication (including digital signatures), confidentiality (encryption), or both. While the list of agency efforts in Appendix A is substantial, it is not intended to be exhaustive. Further, it includes several pilot efforts, which are in the process of getting underway. Thus, the list is intended to be helpful both as an illustration of the growing use of public key technology by Federal agencies, as well as identifying existing or potential future opportunities for companies who sell PKI products or services to those agencies.

Access Certificates for Electronic Services

Federal agency efforts to date have focused on using public key technology for intra-agency, interagency, and agency to trading partner transactions. The largest potential volume of traffic, and the greatest prospects for service delivery, involves transactions with the general public. Recognizing this, and appreciating that the best approach to use public key technology with the public is to devise a PKI that all agencies can collectively use for that purpose to share the costs of a common infrastructure, the General Services Administration (GSA) began working in 1996 on an effort called Access Certificates for Electronic Services (ACES).

The basic ACES model works as follows. A member of the public wishing to get a digital certificate connects through the Internet using Secure Sockets Layer (i.e., with complete privacy) to an ACES Registration Authority. Through that connection and using his or her browser, the individual provides personal information such as name, address, telephone number, and other facts. Once that information transfer is completed, the individual terminates the connection.

The ACES Registration Authority (RA) then verifies the information to ensure that there is an individual with the given name residing at the given address and having the specified private characteristics. Assuming that the verification process confirms the information, a one-time PIN is mailed (an out-of-band transmission) to that person at that address. Upon receipt of the PIN, the individual generates a key pair using the computer's browser, connects using SSL to the ACES Certification Authority, provides the PIN and transports the public key, whereupon the ACES CA issues the certificate which is then placed in the browser. The ACES RA had previously conveyed the same PIN to the ACES CA.

The ACES contracts also provide options for more robust identity proofing, allowing the use of hardware tokens for private keys (depending upon agency needs), the enabling of agency applications to accept ACES certificates, and the performance of other PKI services.

In September and October 1999, GSA made awards to three prime contractors for this project: Digital Signature Trust, Inc., Operational Research Consultants, Inc., and AT&T. Each prime contractor has one or more companies with whom they have partnered; these include America On-Line, Microsoft, Netscape, Entrust Technologies, Baltimore Technologies, Computer Sciences Corporation, VeriSign, and others. A full list can be found at http://www.gsa.gov/aces.

ACES certificates will be free to members of the public; agencies either pay for the certificates for unlimited use, or pay a modest one-time issuance fee (which is competitively determined and may be as low as zero) and then a further fee each time a certificate is used (between $.40 and $1.20 depending upon transaction volume throughout government). Agencies need to make their applications "ACES-enabled" – in other words, to accept ACES certificates for transactions. GSA has formed an ACES Customer Advisory Board among agencies considering ACES to help agencies refine their needs and to aggregate demand for ACES certificates. With time, the list of agencies and applications that are ACES-enabled is expected to grow.

Privacy has been a primary concern in the development of ACES. Information supplied to an ACES RA during the initial registration process is fully protected under the Privacy Act; it is not supplied to any other ACES RA or to any Federal agency or other party. The ACES certificate itself contains no private information, only the subscriber's common name; this means that one individual could obtain multiple ACES certificates, thus making it impossible for the certificate to serve as a "national identification" mechanism. It also means that when the certificate is used for the first time with an agency, the agency will need to further distinguish and authenticate the user through the exchange of one or more shared secrets, such as the user's mother's maiden name or any other fact known to the agency and the user. After this first use, the agency will know exactly to whom the certificate belongs, making a similar process unnecessary when the certificate is used again. This approach is advantageous because it allows an agency to build upon the basic level of authentication afforded in the ACES certificate, to gain whatever level of assurance the agency desires by allowing it to ask for as many shared secrets as needed for the specific transaction to consummate.

Governance of the Federal PKI

Any infrastructure that cuts across multiple agencies requires the cooperation of the affected agencies to make it work. The Federal PKI is no different. While agencies may run their own agency-specific PKI domains to serve their own agency-specific needs, interoperating with other agencies imposes unique requirements and obligations.

Because the Federal PKI has evolved from the bottom-up, that is, from agencies adopting this technology to serve their specific needs rather than having its use prescribed for them, the model of governance which has evolved reflects that paradigm. In 1996, the Federal Public Key Infrastructure Steering Committee was formed under the Government Information

Technology Services (GITS) Board, co-chaired by OMB and the National Partnership for Reinventing Government. The Steering Committee, comprising over 50 members representing over two dozen agencies, has as its focus the promotion of interoperable PKI solutions, the development of common guidance, and the sharing of information so that agencies considering or deploying PKI solutions can benefit from those who have already done so. Participation in the Steering Committee is voluntary. Its activities are published at http://gits-sec.treas.gov and http://cioc-pki.treas.gov.

The Steering Committee formed three working groups to focus particularly on (1) legal and policy issues, (2) business issues, and (3) technical issues. The technical working group, unlike the rest, is chaired by NIST and includes participants from the private sector. Additionally, OMB, in its guidance implementing GPEA, charged certain agencies with particular responsibilities: Department of Commerce in conjunction with the Steering Committee would establish standards and develop technical guidance for the use of digital signatures; the Department of the Treasury would develop policies for financial applications; the Department of Justice would prepare guidance on legal considerations; the National Archives and Records Administration would create guidance on electronic records management; and the General Services Administration would support agencies in their efforts to implement electronic signatures. The breadth of these activities demonstrates the commitment which the Federal government had made to electronic signatures in general, and digital signatures in particular. Further, they serve to reinforce the need for a thoughtful, overarching mechanism to help ensure the interoperable use of such technology.

Beginning in mid-1998, the Steering Committee developed a model for governance of the Federal PKI. This model is best described as "governance by the governed." In other words, those agencies employing public key technology would determine collaboratively how best to ensure they could interoperate efficiently and seamlessly. The model envisioned the creation of a Federal PKI Policy Authority. The Policy Authority would serve to establish the conditions under which an agency-specific PKI would interoperate through a Federal Bridge Certification Authority (FBCA – described below) with other agency-specific PKIs. In essence, the Policy Authority would map the certificate policy of each agency to an FBCA certificate policy, thus allowing an agency to determine whether a certificate from another agency embeds the level of assurance or trust needed for a particular transaction. This model avoids each agency having to develop bilateral relationships and certificate policy mappings with every other agency; instead, that is done once with the Policy Authority.

It is important to note, however, that the model does not compel agencies to use the convenience inherent in the single Policy Authority mapping;

agencies may still strike individual arrangements with others. Rather, this model of interoperability is expected to attract adherents simply because it is so efficient.

In February 2000, the GITS Board announced that its activities would be merged with those of the Federal Chief Information Officers (CIO) Council, and the GITS Board would be disestablished. This occurred in April 2000. The Steering Committee now operates under the auspices of the Enterprise Interoperability and Emerging Information Technology Committee of the CIO Council, and also retains strong ties to the Security, Privacy and Critical Infrastructure Protection Committee of the CIO Council. The Federal PKI Policy Authority is being established under the former committee and is expected to commence operation during Summer 2000. For reference, a copy of the Policy Authority charter is included as Appendix B.

Interoperability of the Federal PKI

Separate from a governing structure is a need to ensure the technical interoperability of the Federal PKI. Three models support such interoperability.

The first model involves the use of a hierarchical structure, where "trust" starts in a single Federal root Certification Authority or Validation Authority, and flows from it down to agency CAs. This is the model that is being very effectively implemented by the Government of Canada in its Federal PKI, and it facilitates interoperability by simplifying certificate trust path creation, making it easier for one agency to accept digital certificates issued by other agencies. Within the U.S. Federal government, however, agencies enjoy a high degree of autonomy and they have a wide spectrum of applications, which make a single "root" unattractive.

The second approach involves the use of CA "trust lists," wherein an agency simply lists those CAs external to it for which it will "trust" certificates issued by those CAs for selected agency transactions. This may be done by listing trusted CAs in a browser, or through other means. While this approach has merit, it imposes a considerable burden on individual agencies to determine which CAs they should trust, at what levels the certificates issued by those CAs should be trusted, how those CAs are identified as "trusted" in agency application software, and how to ensure the "trust list" is not inappropriately altered to include CAs which should not be on the list. Moreover, when a PKI employs certificates issued at multiple levels of assurance rather than a single level, the trust list model becomes substan-

tially more complex, requiring the management of a different trust list for each level.

The final approach, which is the one being implemented under the auspices of the Steering Committee, is to design, implement and operate a Federal Bridge Certification Authority (FBCA) to act as a non-hierarchical "hub." Agency CAs would receive permission from the Federal PKI Policy Authority to interoperate with the FBCA under terms that were mutually negotiated and accepted. Every CA that interoperates with the FBCA would be able to interoperate with each other. It is useful to describe this process.

When one agency (the "recipient") receives a transaction from another (the "sender") that is digitally signed using a private key corresponding to a public key in a certificate issued by the sender's CA, the recipient's application software must do three things to allow the transaction to consummate. First, the recipient must determine whether the certificate originated from a CA that has a trust relationship with the CA in the recipient's agency. This is done by creating what is called a "trust path" of certificates from the CA in the recipient's agency, through the Bridge CA, and ultimately to the CA in the sender's agency. Second, the recipient must determine whether the certificate has sufficient trust for the transaction (For example, was the individual required to appear in person and to produce picture identification cards to get the certificate?). This trust determination is done using the policy mappings made by the Federal PKI Policy Authority and instantiated in the certificates issued by the FBCA to the agency CAs. Finally, the recipient must determine that none of the certificates in the trust path – including the certificate offered for the transaction – has been revoked. If all of these conditions are met, the recipient can accept with confidence the certificate and allow the transaction to consummate. The FBCA, in essence, creates the environment, which allows all of those determinations to be made efficiently and with confidence.

At the same time, it should be emphasized that when an agency acts as a relying party (that is, when it is determining whether to accept a certificate issued by another agency), the relying party agency is not required to use the Policy Authority mapping. It may employ whatever mapping it determines appropriate. This preserves agency autonomy. Moreover, the FBCA approach described above can be adjusted to accommodate a "trust list" approach, by having the FBCA digitally sign and post one or more such lists. This would permit a hybrid model that is likely to accommodate a broader spectrum of commercial products.

Lead responsibility for designing, implementing and operating the FBCA resides with the Federal Technology Service of GSA, the same organization responsible for ACES. The Steering Committee, NSA, and NIST pro-

vide technical and programmatic oversight. The FBCA will come into existence in two phases. In the first phase, the FBCA has been implemented as a prototype, which went operational for testing purposes on February 8, 2000. The prototype has two CA products supplied by Cybertrust and Entrust, which interoperate within the FBCA itself and thus support interoperability with any agency CAs that can interoperate with either of those products. (With the acquisition of Cybertrust by Baltimore Technologies, the Cybertrust CA is being replaced with the Unicert CA.) The production version will build upon that architecture to include additional CA products within the FBCA so that full interoperability is supported with any CA product or service an agency may select for its use. Indeed, this is the unequivocal goal of the FBCA: whatever CA product or service an agency selects, they will be able to interoperate using the FBCA. Depending upon the availability of funding being sought for this purpose in the Fiscal Year 2001 budget, the production FBCA should be operational by late 2000.

The FBCA Prototype and Electronic Messaging Association Challenge 2000

The first use of the prototype FBCA was demonstrating interoperability during the Electronic Messaging Association (EMA) Challenge 2000 April 6th through 8th, 2000. The prototype FBCA supported S/MIME messaging among several disparate PKI domains having a total of five different CA products, five different X.500 directory products, and two e-mail clients modified in different fashions. The domains for which interoperability was successfully demonstrated are: (a) two Entrust CAs at NIST; (b) one Entrust CA run by the Government of Canada; (c) three Entrust CAs at the Georgia Tech Research Institute; (d) one Entrust CA at the National Aeronautics and Space Administration; and (e) a Cygnacom Solutions CA run by the National Security Agency which itself is a “bridge” with which three groups of CAs are cross-certified, one being three hierarchically organized Spyrus CAs, another being three hierarchically organized Motorola CAs, and the final being four meshed Entrust CAs.

The EMA Challenge demonstration illustrated interoperability on several levels – between CAs, between directories, and between e-mail clients. The EMA demonstration used Eudora and Microsoft Outlook e-mail clients: the former was modified using the Entrust toolkit and specially designed plug-in libraries created by two Federal agency contractors, Cygnacom Solutions and JGVanDyke; the latter was modified using the Entrust toolkit. Each client created a certificate trust path between the domain of the

recipient and the domain of the sender, and then processed the trust path (i.e., verified the signatures of the certificates, and determined whether any certificate in the trust path had been revoked). This was done as part of validating the signature of the sender on the e-mail. Trust paths tested were up to seven CAs in length. Directory chaining (X.500 Directory System Protocol, called "DSP") was used between directories, with the Lightweight Directory Access Protocol (LDAP) employed by the e-mail client to access its local directory. The model does not require X.500 DSP; LDAP with referrals could be employed if the client software were modified for that purpose. While the FBCA will also support the additional functionality of policy mapping between disparate PKI domains, and certificate discovery and trust path creation and validation for encryption, those capabilities will be demonstrated subsequent to the April EMA Challenge.

Eudora was selected as the e-mail client for the specially designed plug-in libraries because the effort required to include the certificate path creation and processing functionality was not excessive; the relevant libraries have been made publicly available at:

(1) Certificate Path Development Library:
http://www.cygnacom.com/cpl/
(2) S/MIME Freeware Library:
http://www.armadillo.huntsville.al.us/software/smime
(3) Certificate Management Library:
http://www.armadillo.huntsville.al.us/software/certmgmt/index.html

Since Federal government users employ a wide variety of e-mail products, and since plug-ins can be complex and difficult to manage in widespread applications, efforts are underway to address including such functionality in the native code of e-mail products. Indeed, it is hoped that S/MIME messaging represents a crosscutting Federal agency use of PKI, which may prompt faster adoption and use of this technology than any other single application.

Public Key Technology and Critical Infrastructure Protection

A basic step in protecting any critical infrastructure is knowing with whom you are dealing. If you cannot authenticate remote users, the infrastructure is susceptible to attack on a fundamental level.

The National Plan for Critical Infrastructure Protection, developed pursuant to Presidential Decision Directive Number 63, recognizes that public key technology plays a vital role in user authentication, for the reasons cited above. Thus, an agency decision to employ a PKI for an application may be premised on more than just efficiency, long-term cost savings, scalability, or extensibility; it may also be premised on the need to ensure that the agency's electronic infrastructure is properly protected.

The Future

Trying to predict what will happen in the information technology realm is an exercise fraught with great risks. This is especially true with respect to a technology that is evolving as quickly as public key cryptography. Nonetheless, there are certain undeniable premises or trends, which may provide important and useful clues.

First is the fundamental need for strong authentication over a wide range of applications that use electronic transactions. As explained above, public key technology meets this need better than any other single technology, and combined with other elements such as biometrics, can create a very secure environment important to e-commerce, e-government, and critical infrastructure protection.

Second, Federal agency use of public key technology is growing quickly both vertically (within organizations) and horizontally (across organizations). This growth is occurring from the bottom up, employs multiple products, and promises to continue in that manner.

Third, Federal agencies and OMB recognize the need to create a governing structure, which will facilitate interoperability among the disparate agency PKIs, and ultimately support interoperability with external organizations in an efficient manner. The Federal PKI Policy Authority and Federal Bridge Certification Authority respond to this need.

Finally, to sustain growth requires several things: products must become more interoperable, standards must evolve to stable form, and application software must fully employ the capabilities which a PKI provides for checking certificate status and assurance before allowing a transaction to consummate. Fortunately, these things are occurring, through the efforts of the Federal government, private companies, educational and research organizations, and international bodies.

Credits

This report is the product of many people associated with the Federal PKI Steering Committee. While it is impractical to list all who contributed, special thanks are due to the following individuals who contributed assistance well beyond just providing information on the activities of their own agencies: William Burr of the National Institute of Standards and Technology; William Kelly and Arthur Purcell of the U.S. Patent and Trademark Office; Eugene McDowell of the National Oceanic and Atmospheric Administration; Johnny Sumners of the Department of the Treasury; Dinesh Kumar of the Social Security Administration; and Joseph Mettle and Denise Silverberg of the National Security Agency.

Appendix A: Federal Agency PKI Efforts

This appendix describes the efforts of Federal agencies employing public key technology for authentication (digital signatures), confidentiality (encryption), or both. This is not intended to be an exhaustive list, but rather one that covers important activities illustrating the depth and breadth of PKI use within Federal agencies. Moreover, the order in which the efforts appear does not connote significance. Further, the list does not include many other agency applications which use only Version 2.0 of SSL for session encryption; rather, the list focuses on applications that result in the issuance of end-user certificates, which can include Version 3.0 of SSL (where cross-authentication is done). Finally, a tabular summary of the efforts described below can be found at the end of the appendix.

1. Department of Agriculture/National Finance Center (NFC)

NFC provides a wide range of financial services to Federal agencies, including payroll and other personnel management activities. One such application is the Purchase Order Invoice System (POIS) for the Rural Development Agency (RDA) and the Farm Services Agency (FSA). NFC processes approximately $200 million per annum in Purchase Order Payments for these two agencies, and employs PKI for this purpose.

To obtain a digital signature certificate, RDA and FSA users are required to appear in person before a Registration Authority (RA) with two forms of identification, at least one of which must have a picture. The user signs an agreement, witnessed by the RA. The RA then forwards the request to NFC, who runs the CA and issues the certificate. The CA employs COTS software (Entrust). Approximately 400 RDA and FSA employees have been issued digital certificates.

In the POIS, RDA and FSA employees digitally sign purchase orders and send them via the Internet to NFC. NFC authenticates the signature on a purchase order, archives a copy with the digital signature, and then forwards the purchase order to the mainframe for processing. The purchase order and digital signature are stored for three years. Confidentiality is obtained using a Virtual Private Network employing Entrust certificates used to secure the session from the user's desktop to NFC's server. Since POIS began using digital signatures, RDA and FSA have seen a reduction in processing time from two to four weeks, to one day, with rejection notices being received the same day. Penalties from vendors for late payment have been reduced by 75%.

NFC is in the process of standing up another CA, which will be suitable for supporting agency personnel activities, such as PKI-based access to employee payroll and other records. Since NFC is a service-provider agency, its ability to offer this service will be affected by whether agencies are willing to pay for it. NFC is also working within the Department of Agriculture to provide PKI services to other offices. Further, NFC is expanding its efforts to provide web server and web client certificates to meet agencies' needs for Secure Sockets Layer (SSL) encryption.

2. *Department Of Labor/Bureau of Labor Statistics (BLS)*

A prototype Centralized Internet Data Collection facility has been established and uses digital certificates for user identification (authentication). This system is designed to collect data from respondents to BLS surveys. VeriSign certificate services were chosen for the pilot. The goal is to allow respondents to use industry standard browsers (Microsoft and Netscape) to communicate data to BLS with a minimum of BLS support for the client side. The project is in the internal testing phase. It is intended ultimately to support multiple applications beyond data collection.

3. *Department of Commerce/National Institute of Standards and Technology (NIST)*

NIST currently uses over 200 paper forms, most of which are generated using a COTS forms package. The form package is just used to fill and print out the paper forms. Then the paper is routed, approved, and data from the forms is keyed into administrative systems. After that, the paper is often filed. This project's objective is to replace the paper process with an all-electronic system that uses a "workflow" package. Paper will be replaced by electronic messages or forms, which are entered by NIST staff, routed automatically where they have to go, and approved by appropriate NIST managers and administrators. Data will be automatically captured for administrative databases, all without printing any paper. Digital signatures and possibly encryption will be used for these processes.

NIST has two campuses located in Gaithersburg, Maryland and Boulder, Colorado with about 3,000 seats and a very diverse environment. Many personnel are bench scientists, who use a great variety of workstations and servers. Most administrative systems on desktops employ Windows 95, 98 and NT and the server environment is becoming largely Windows NT based. Therefore, the desktop part of the application will be required to run on Windows platforms, but the servers may be Windows or non-Windows based. NIST technical staff members have substantial latitude in the

systems and software they choose to use on their desktops. For example, while Eudora is the "standard" NIST e-mail client, many other clients are used.

Most private keys will be held in encrypted form on the keyholder's hard disk, and decrypted under a pass-phrase. However, some positions will require hardware tokens, or possibly biometric activation of keys. The PKI subscriber universe will be NIST employees, with guest researchers and some contractors who work on the two NIST campuses.

NIST expects to use S/MIME v3 mail clients that support separate signature and encryption certificates, which would facilitate encryption key recovery, if needed. However, at this point digital signatures are the main focus of the effort; whether encryption is needed for routine administrative actions has not yet been determined.

To execute this effort, NIST conducted a competitive procurement and has awarded a contract to an integrator under the Department of Commerce COMMITS GWAC procurement vehicle. NIST will install an Entrust CA, automate four frequently used, relatively low risk actions by winter of 2001, and pilot them on 100 desktops. In phase two, NIST will install these applications on approximately 3,000 NIST desktops in the summer of 2001. The infrastructure will then exist to automate the bulk of NIST's internal business processes.

NIST expects to achieve significant savings by having staff perform administrative actions directly that are now being done by secretarial and administrative staff, eliminating re-keying of information from paper to databases, as well as making the administrative process faster, simpler for staff, and more manageable. To realize these benefits fully, it will be necessary to review and reengineer many business processes at NIST to incorporate them into the new system.

4. *Department of Commerce/United States Patent and Trademark Office (USPTO)*

The USPTO PKI is being implemented as part of an integrated information technology infrastructure to provide for both internal and external uses of public key technology. This enables the USPTO to have a single, highly scaleable security infrastructure to support both internal and external applications regardless of risk level. The implementation of a single PKI will provide security and authentication for a wide range of business applications rather than providing separate, stovepipe security solutions for individual applications.

The USPTO PKI will ultimately support secure and authenticated communications and commerce with the USPTO patent applicant community, Registered Patent Attorneys and Patent Agents, international business partners including other Intellectual Property Offices, Patent and Trademark Depository Libraries, USPTO employees and support contractors, and others with whom the USPTO does business which requires guarantees of authenticity and confidentiality.

To obtain a digital certificate, identity-proofing requirements vary. For independent inventors, presentation of two forms of identification to the USPTO or to a Notary is needed. For Patent Attorneys and Agents, identity records and signature specimens, which the USPTO keeps for each such party, are used. For employees of the Patent Attorney or Agent, the Attorney or Agent verifies identity. The USPTO is considering partnering with the U.S. Postal Service and the Patent and Trademark Depository Libraries to serve as Local Registration Authorities.

The USPTO employs Entrust software, and operates the Certification Authority (CA) directory and application servers in security zones protected by firewalls and further secured by versions of compartmented mode workstation software. There are hot and cold backups for the CAs in case of the failure of the primary CAs and the directory servers are implemented in a manner to permit rapid restoration in event of failure or data corruption.

The Entrust client software on the user's computer protects the private keys, but at the user option, the private key and certificate may be transferred to a smart card or other token compatible with the software. At the USPTO, the CA software escrows the encryption key. The USPTO CA private keys are protected using commercially available technology for physical and network security.

The initial PKI started as a pilot that has evolved into a production system called the Patent Application Information Retrieval (PAIR) system. The PAIR system permits authenticated access to patent application information using a digital signature, and establishes an encrypted session (from the user's desktop to the USPTO server) for confidentiality. The USPTO must maintain the confidentiality of pending patent applications. The USPTO deployed PAIR to improve responsiveness to applicant requests for patent application status information.

A second effort is called the Electronic Filing System (EFS) and is in the pilot phase. EFS supports the authoring and secure and authenticated filing of patent applications. The EFS pilot makes use of both signature and encryption to preserve the authenticity, integrity confidentiality, and non-repudiation of patent application data submissions. To date, the USPTO

has received five electronic patent applications through the Internet. The USPTO will expand the pilot in August 2000 by including additional types of transactions and more pilot participants. Full production is planned for February 2001.

To date, the USPTO has issued over 570 certificates. The same certificate can be used to submit patent applications electronically or request information on the status of the patent application. Given the initial highly positive response and the expressions of interest by patent practitioners, the USPTO expects that between 6,000 and 10,000 certificates will be in use before the end of 2000.

Separate from PAIR and EFS, USPTO anticipates developing PKI-based security services for the following automated information systems and information technology infrastructure services: (a) Patent Application Capture and Review (PACR); (b) PCT Operations Workflow and Electronic Review (POWER); (c) International Priority Document Exchange (IPDE); (d) Office Action and Correspondence System (OACS); (e) Tools for Electronic Application Management (TEAM); (f) Enterprise-wide Login (EWL); (g) Patent and Trademark Assignment System (PTAS); (h) Patent and Trademark Depository Libraries (PTDL); (i) Human Resource Information System (HRIS); (j) Revenue Accounting Management (RAM); (k) Trademark Work-At-Home; and (l) Patent Work-At-Home.

To date, a total of over $4 million has been spent on the USPTO PKI. This represents a considerable investment, but USPTO believes that it will translate into substantial savings and improved service delivery. For example, when a patent application is filed containing nucleotide or amino acid sequences, it may contain many thousand pages of sequence information. The physical mass of paper is difficult to maintain and use. The implementation of EFS permits the electronic filing of these sequence listings in place of the paper as part of the legal patent application record and saves the customer and USPTO the time and expense of providing a voluminous paper copy. The PKI services permitted the USPTO to hold only the electronic file as the official record. Another area of savings is due in part to the "Intellectual Property and Communications Omnibus Reform Act of 1999," which was signed into law on in November 1999 and which requires publishing of the filed U.S. applications in specified circumstances but permits redaction of portions of the applications. The submission of applications in electronic form will substantially reduce costs for printing and redaction of these patent applications. Currently, the USPTO spends $36 million annually to perform this function.

The use of PKI promises improved service delivery in response to USPTO customer expectations. Since 1994, the USPTO applicant and attorney com-

munity has asked for better access to patent application status information. Improving responsiveness for answering status questions is one of USPTO's Customer Service Commitments that are measured annually. Based on customer input, the USPTO established a customer service commitment in 1995 to provide applicants with the status of their application within 30 days. The 1999 customer satisfaction rate was only 38 percent for this commitment. PAIR was implemented to address this need through convenient and prompt transactions over the Internet, while meeting the requirements for authenticity and confidentiality. By contrast, non-automated status information requests are by letter or phone and are time consuming for both the customer and the USPTO, so the implementation of PAIR will save substantial time for both USPTO and its customers. In January 2000, USPTO customers submitted nearly 24,000 queries to obtain the status of their patent application – which means that the USPTO did not have to prepare 24,000 post cards to send to patent applicants with the current status of their application. This also enables the USPTO to reduce the "30 day" customer service commitment for patent application status to seconds.

5. *Department of Defense (DOD)*

DOD is employing public key technology to serve a broad array of activities. Since DOD employees (military and civilian) represent over 50% of the Federal workforce, DOD efforts have particularly significant impact.

The Deputy Secretary of Defense and other senior DOD officials promulgated policy in 1999 calling for all DOD military and civilian employees to be issued PKI-enabled Smartcards by the end of 2002; to employ S/MIME for secure and authenticated unclassified messaging; to use digital certificates issued by DOD CAs and by vendor CAs to support a wide variety of electronic transactions between DOD and its vendors; and to test different PKI interoperability models including one which supports interoperation using the FBCA. DOD efforts are proceeding in each area.

The traditional PKI is based on a hierarchical design, with a single Root CA at the top of the hierarchical tree, followed by subordinate CAs (which receive their certificates from the Root CA), and subscribers (which receive their certificates from the subordinate CAs). This architecture requires absolute trust relationships between the Root CA and the subordinate CAs, so it is normally viewed as working within a single enterprise. Between enterprises, however, a peer to peer relationship is more common, and DOD is supporting an important test of this architecture that is related to the FBCA.

The National Security Agency (NSA), in cooperation with NIST and several PKI product suppliers and integrators (including Entrust, Cygnacom Solutions, Motorola, J.G. Van Dyke and Associates, Booz-Allen Hamilton, and Spyrus), is developing a PKI system referred to as the Bridge Certification Authority Demonstration Project (BCA Demonstration). The BCA Demonstration covers both encryption and digital signatures.

The central component in the BCA Demonstration is a CA developed by Cygnacom, which is networked and cross-certified with CAs from Motorola, Entrust, and Spyrus, which themselves have subordinate CAs that issue certificates to end-users (subscribers). The BCA Demonstration uses an EUDORA S/MIME e-mail client with special additions that make it capable of (a) discovering (creating) certificate trust paths between subscribers; and (b) validating the certificates in the trust path. Ultimately, the client will also contain code to process the certificates in those trust paths in accordance with X509 requirements, employing the mappings for certificates in different PKI domains through the policy mappings extension fields. Thus, the BCA Demonstration focuses on enabling client software to use the functionality, which a Bridge CA provides. (Note: Use of the BCA Demonstration in conjunction with the Federal Bridge Certification Authority is discussed in the body of the report.)

In addition to these efforts, the military services are pursuing PKI applications under the overall DOD PKI. These efforts are reported separately below.

a. Department of the Navy (DON): The DON PKI implementation strategy invokes an aggressive plan to place cryptographic smartcards in the hands of all Navy and Marine Corps employees by the end of CY 2002 using Commercial-off-the Shelf (COTS) technology. By moving as quickly as possible to issue and use hardware-based certificates, the DON will increase security and avoid the additional costs and burdens associated with issuing and maintaining software-based certificates. More importantly, this convergence of smartcards and PKI will provide each Navy and Marine Corps employee with a single card – the DOD Common Access Card (CAC) – which functions not only as a "cyber identity" (containing digital certificates for both authentication and data encryption purposes), but also as a mechanism to achieve access authentication to network resources, web-enabled applications, while serving as an individual's personal identification card that allows building access.

On November 10, 1999, the Deputy Secretary of Defense (DEPSECDEF) assigned the Department of the Navy to "take the lead in preparing a smart card Operational Requirements Document" and "serve as Chairperson for the Smart Card Senior Coordinating Group" for DOD. Additionally, the

DON led a Services / DOD Agencies effort to address the requirement of Section 374 of the FY 2000 National Defense Authorization Act (Public Law 106-65, October 5, 1999) to submit a report addressing the "Consideration of Smart Cards as the DOD PKI Authentication Device Carrier." This report was submitted to the Secretary of Defense in December 1999.

The U.S. Navy has approved 94 Local Registration Authorities (LRAs) for registering subscribers to receive Class 3 DOD PKI certificates. The LRA is the focal point for the identification and registration of Navy users into the PKI. Over 2,000 certificates have been issued within the Navy, including approximately 1,200 identity certificates, 600 confidentiality certificates, and 350 server certificates. Additionally, the Navy and Marine Corps will leverage the LRA functionality provided by deployment of the integrated DOD Real-time Automated Personnel Identification System – LRA workstations.

The Marine Corps will serve as the RA for their personnel, including service members civilian employees, and contractors. The Marines have established two major RAs; primary RA at Marine Information Technology Network Operations Center in Quantico, Virginia, and secondary RA at the Marine Detachment located at the Defense Finance and Accounting Service office in Kansas City, Missouri. Installation of a total of 134 LRAs is in progress. To date, the Marines have issued over 500 certificates and are currently using Secure / Multipurpose Internet Mail Extensions (S / MIME) e-mail where practical; other applications under development involving authenticating network devices using web server authentication / confidentiality.

The DON is overseeing four PKI-smartcard pilots: (1) an in-house DOD PKI smartcard Windows 2000 effort within the DON CIO office using a Microsoft CA to accomplish secure network logon and allow the use of DOD certificates to access secure web sites and support secure messaging systems; (2) an effort under the Assistant for Administration in the Office of the Under Secretary of the Navy testing digital signatures as replacements for actual personnel signatures concerning the use of Official Representation Funds; (3) the Space and Naval Warfare Systems Command which is evaluating COTS web servers and e-mail and web clients to develop the procedures necessary to implement the DOD PKI for these products; associated implementation procedures are posted to the Navy INFOSEC Web Site at http: / / infosec.navy.mil / PKI; and (4) Commander-in-Chief Pacific Fleet who is testing PKI in a limited shipboard environment.

Implementation efforts for several PKI-enabled applications within the DON are also underway. Specifically, the Naval Supply Systems Command is PKI-enabling several acquisition programs to provide added se-

curity for users to exchange acquisition-sensitive information over the Internet. Further, the Naval Air Systems Command is PKI-enabling the Naval Aviation Logistics Data Analysis Integrated Data Environment via application layer security and is also using PKI to exchange acquisition data between the F-18 Program Office and contractors.

b. Department of the Army: The Army's overall strategy to achieve the target DOD PKI is linked intrinsically to the overall DOD strategy. Key to the successful implementation of both strategies is the ability of the Army to begin immediately to leverage the existing PKI capabilities afforded by commercial technology. The DOD PKI strategy recognizes that traditional government off-the-shelf (GOTS) implementations will not be able to keep pace with an information assurance strategy that is based on commercial technology and services. It further recognizes that the DOD PKI must, to the greatest extent possible, employ open standards based on commercial products and services that can keep pace with technological advancements and the constantly evolving applications and standards that are inherent in the information technology environment. The DOD PKI must do this while still maintaining the appropriate levels of security for the information being protected.

To accommodate the DOD strategy and to ensure that the Army's implementation of PKI is consistent with the DOD approach, an Army PKI vision has been developed that prescribes the use of COTS products and describes a single key management infrastructure as its end state. Simply stated, the Army PKI vision is:

> *By 2005, all Army personnel will have the capability to digitally sign and/or encrypt all information exchanged in an open network environment through a single key management architecture.*

To help convert this vision into reality, in late September 1999, the 5th Signal Command, United States Army Europe (USAREUR) and the Defense Information Systems Agency (DISA) launched a DOD Medium Grade Service (MGS) Pilot Project. USAREUR is leading the Army implementation efforts by securing COTS e-mail (Microsoft Outlook 98) with DOD Class 3 (Medium Assurance) certificates for signature and encryption. On 20 September 1999, USAREUR and DISA provided LRA training to 22 personnel in Mannheim, Germany. The LRA performs a key function: verifying individual identity and requesting individual certificates from the CA. The Army RA authorizes LRA certificates, revokes all types of certificates, and manages the Army's block of numbers that uniquely identify certificates. The Army will maintain RAs in two organizations. The Army Signal Command will issue certificates for servers, while the RAs for personnel certificates will reside in the Office of the Director of Information Systems for

Command, Control, Communications and Computers.

USAREUR put a new spin on the "train the trainer" concept. As soon as the LRAs were operational, the USAREUR Information Management Officers (IMOs) were issued their individual certificates and were then trained on the procedures for importing the Class 3 certificate into their commercial e-mail product. The IMOs are working with the LRAs in their geographical area to register end users for their DOD PKI certificates. The IMOs are providing the procedures and "hands on" assistance for enabling email with DOD PKI. Over 1200 individuals in USAREUR have been registered and approximately one-third are already using their certificates to sign and encrypt e-mail. By September 2001, the goal is to have approximately 20,000 certificates issued.

c. Department of the Air Force: There are numerous applications running with SSL under the DOD PKI initiative. For specific E-commerce applications, the Air Force is using approximately 60 servers and has enabled the Electronic Posting System, which is a contract submission/evaluation process. Additionally, the Air Force is using wide area workflow and electronic document access (a DOD-wide system), both of which are PKI-enabled. These represent three of the five systems involved in the Air Force's e-commerce start-to-finish processes. The other two systems – automated business services and standard procurement system – are being re-engineered to accept certificates.

6. *Department of Energy (DOE)*

DOE has several ongoing applications, which employ PKI. There are five CAs (using Entrust software) cross-certified among themselves at DOE national laboratories and field activities, with over 2,000 certificates issued to DOE Federal and contractor employees in support of secure and authenticated e-mail (S/MIME), file management, data transfers, and personnel management functions. An additional 500 certificates are expected to be issued in FY 2000. DOE is in the process of developing a certificate policy and determining the architecture for headquarters which will interoperate with the existing laboratory and field activity PKIs. Additionally, DOE is performing a pilot effort using a Cygnacom Solutions CA to provide certificates, which would be used by a GELCO Travel Manager system in support of travel requests and travel claims processing.

7. *Environmental Protection Agency (EPA)*

EPA has numerous applications, which employ or are likely to employ PKI. These applications are in various stages of completion, and are discussed separately below.

a. Under the Resource Conservation and Recovery Act, companies which ship hazardous waste for treatment, storage or disposal must complete and sign a Hazardous Waste Manifest that allows shipment tracking. The shipping agent must also sign the manifest, as well as the recipient upon delivery. EPA is pursuing a pilot effort that would employ cryptographic processes for these signatures and for authentication purposes, but not for confidentiality since the manifest data are publicly available.

b. Under the Toxic Substances Control Act (TSCA), there are multiple requirements obliging companies to report information to EPA; these include Health and Safety Submissions (TSCA sections 4 and 8), Premanufacture Notices (TSCA section 5), and Export Notices (TSCA section 12b). EPA is currently testing electronic submissions under these provisions, where submitters will digitally sign PDF documents or forms and submit them to EPA either over the Internet or on a diskette. Planning for this effort began in 1996 with EPA hosting a series of "open sessions" designed to solicit feedback for the conditions and procedures under which electronic submissions would be acceptable for both industry and EPA.

c. The Integrated Grant Management System (IGMS) uses Lotus Notes for e-mail, and to develop workflow based applications for forms routing and grant negotiation. Notes Release 5.0 provides an S/MIME compliant PKI capability as a core function, and IGMS employs this capability. IGMS is a paperless, programmatic and administrative system, which fully automates the grant process from cradle to grave. For the first time, IGMS allows grantees to do business with EPA totally electronically, and support electronic grant approval and management within EPA. IGMS strengthens EPA's relationships with environmental partners, by providing tools that support collaboration on environmental programs. It also improves the speed and user-friendliness of the grant process, increases post award and closeout management, and improves EPA and grantee availability of grant funds.

d. Under the Clean Water Act, companies are required to report discharges of pollutants into open bodies of water under their National Pollutant Discharge Elimination System permits. In some states, such as New York, the process of negotiating these permits with industry is delegated to state regulatory agencies. The reports, called Discharge Monitoring

Reports (DMRs), include pollutant content of effluent streams as well as other parameters such as temperature and pH, and are submitted usually on a monthly or quarterly basis.

Electronic reporting of DMRs would provide several advantages, including providing the data in electronic form for easier interpretation and use by EPA or a state; higher data integrity; and stronger ability to bind the identity of the submitter to the data, which promotes accountability and will facilitate enforcement actions should they be necessary. To test the feasibility of electronic reporting of the DMR and to gain information useful in writing electronic reporting rules for other types of compliance reports, EPA has sponsored a test of web-based electronic DMR reporting in New York. Seven companies and local waste water treatment facilities who are required to submit the New York State version of the DMR to the New York State Department of Environmental Conservation responded to an invitation to participate in a pilot test of electronic DMR reporting which was conducted from June to November, 1999. Encrypted Secure Sockets Layer (SSL) was used to encrypt login IDs and passwords which the pilot participants used to gain access to the pilot Web site, and also to protect a client-authenticated session between the Local Registration Authority administrator and the Certification Authority server across the Internet, but no encryption of stored data or documents occurred in the pilot. A digital signature was applied to each electronic DMR form.

EPA selected E-Lock Technologies, Inc., to provide the PKI services for the pilot. These services included a web site to collect identity information from the pilot participants, and to allow the Local Registration Authority administrators in the New York State Department of Environmental Conservation to approve, or approve with modifications, the enrollments submitted by the pilot participants. The Certification Authority service was also on a Web site; a total of 20 certificates were issued to seven participating organizations for the pilot. The product suite, Assured Transactions (ATS Version 2.1) allowed a digital signature to be applied to an Adobe Acrobat Exchange Version 3.01 form. Private keys were protected on hardware tokens (GemSAFE Smartcards), and client platforms ran Netscape Navigator on Microsoft Windows 95, 98 or NT operating systems.

The Central Receiving (CR) Project has recently been established to respond to internal (e.g., Reinventing Environmental Information) and federal-wide mandates for electronic reporting (e.g., the Government Paperwork Elimination Act). A key goal of the project is to create a single, uniform approach for the authentication of electronic submissions of environmental compliance reports. At the center of this approach will be an EPA PKI consisting of the technical infrastructure, organizational practices, policies, and possibly regulations needed to manage the identity proofing, and cer-

tificate issuance and maintenance. EPA is conducting requirements and risk analysis and using this information as the basis for designing a prototype PKI for testing later this year. The goal is to complete the analysis and testing by fall 2000 and codify the CR architecture in a final design specification by early 2002. EPA plans to procure PKI products and services for the CR prototype through the GSA ACES contract.

8. *Federal Deposit Insurance Corporation (FDIC)*

FDIC is using two separate PKIs. One is a low assurance PKI, used for a number of SSL web based applications on the FDIC extranet with FDIC's member institutions and other parties' external to FDIC such as state and federal regulatory agencies. Browser certificates are used to control access to the extranet web server. The second PKI is the FDIC core medium assurance PKI. This PKI covers FDIC employees and some contractors, and is being used for digitally signing and encrypting electronic travel vouchers to facilitate processing. Each PKI is discussed further below.

The extranet PKI uses 128-bit RSA encryption via SSL, and employs Entrust WebCA software. The core PKI uses dual certificates, one for signature and one for encryption, and uses software supplied by Entrust (Version 3.0c1), with the ICL X.500 version 7.B directory. FDIC is in the process of deploying a Microsoft Certificate Server for Outlook web access. The operating environment consists of IP version 4 and Cisco Systems routers; LDAP (port 389) is employed for directory access.

The extranet PKI currently has approximately 2,000 certificates issued. Of these, approximately 600 are in active use. The core PKI has over 3,500 certificates deployed. This number will increase to 10,000 within the next six months. Each FDIC Federal employee (approximately 7,000) has a directory entry.

The extranet PKI uses software based protection mechanisms (web browser certificates). The core PKI currently uses two forms of tokens, software and smart card. FDIC will explore migrating all core PKI users to a combined smart card and building badge.

9. *General Services Administration (GSA)*

The Federal government mechanisms for posting Requests for Proposal (RFP) and receiving vendor responses has been reinvented using public key technology. Under the *Federal Paperless Transactions for the Public* pilot project, the General Services Administration, Federal Technology Service

(FTS) digitally signed the FTS2001 RFP and posted it on their web site along with a downloadable application to check signature validity and document integrity. Subsequently, the same project provided a means for vendors to propose electronically on the FTS2001 contract by signing their proposals using digital signatures. Finally, contract award was also conducted in a paperless environment using the same digital signature capability. In this acquisition process, for the first time, paper proposal submissions were not required. Subsequent task orders and proposals are also being processed electronically using the same technology.

To illustrate the savings, which this new approach afforded, it is useful to describe how the non-electronic process worked. Offerors on large contracts were required to submit both electronic and paper copies of their proposals, many that ran to thousands of pages. The electronic copy was used for evaluation; however, the paper copy carried the official signature of the offeror's authorized official. This required the government to carefully compare the contents of the electronic and paper submissions since any discrepancy could affect the entire contractual agreement. By using digital signatures, the electronic copy became the "official," binding copy and the requirement for a paper submission was negated. Thus, the government was released from the burden of having to compare the two submissions, and the offerors are released from submitting reams of paper in support of the proposal.

Tangible benefits include savings to the government in labor hours expended to validate the electronic copy of the proposal against the paper copy. For FTS2001, rough estimates indicate savings of approximately $1.5 million covering 52,000 man-hours. The amount of paper that would have been processed, if stacked, is estimated to have reached 12 stories.

The FTS Office of Information Security, which put together a secure architecture using commercial off-the-shelf products available from private industry, provided the technology that enabled this improved business process. They forged partnerships with various vendors to develop an infrastructure that is FIPS compliant and satisfy principles set forth by the General Accounting Office for digital signatures. The resulting application provides authentication, data integrity, and non-repudiation of the electronic proposal submission enabling, for the first time, a valid paperless transaction.

Separate from the paperless contracting effort, GSA's Office of Governmentwide Policy has partnered with CommerceNet, a non-profit consortium of Internet companies, on an interagency public/private pilot to promote interoperability between electronic catalogs across the Internet.

Several agencies have implemented electronic catalogs to allow government buyers to purchase supplies and services from common contract vehicles, such as the GSA Schedule (GSA Advantage), the NASA Scientific and Engineering Workstation Procurement (SEWP), and the DOD E-Mall. The Electronic Catalog Interoperability Pilot, conducted in two, demonstrated capabilities for linking these catalogs, as well as commercial catalogs to provide a single interface to the procurement personnel.

Phase one of the pilot delivered the foundations of an interoperable catalog framework using the Extensible Mark-up Language (XML), an open standard for describing data utilized in business transactions. The initial phase also demonstrated that it was possible to search and glean product information from multiple disparate catalogs through the application of technologies that offered great promise form the reducing the time and cost of procurement.

Phase Two built upon the successes of Phase One by enhancing scalability, including registry services to locate products, markets, and suppliers, and providing a demonstrable security framework for end-to-end electronic commerce.

The security framework used asymmetric key pairs and X.509 certificates for authentication, validation, and digital signatures. Server applications were PKI enabled using the Entrust toolkit. The Certification Authority for the pilot was hosted at GSA's Office of Electronic Commerce. Remote nodes were secured using the RadGuard virtual private network (VPN). NDS Americas issued Smartcards with PKI capabilities to the pilot participants in early January 2000.

The pilot authenticated procurement personnel at multiple agencies via a smartcard, applied digital signatures to purchase orders and secured procurement communications through VPN tunnels. The pilot demonstrated the potential for reducing the cost of procurement for items under $25,000 in a secure, interoperable environment that allows multiple agencies to leverage their individual relationships with suppliers.

CommerceNet partners contributed extensive resources to develop interoperable solutions based on XML and secured using PKI. The findings from the pilot will be made public through an independent evaluation report to be issued by PricewaterhouseCoopers.

In addition to these efforts, GSA is also executing the Access Certificates for Electronic Services (ACES) effort and the Federal Bridge Certification Authority effort; those efforts are described in the text of this report and so are not repeated here.

10. *Department of Justice (DOJ)*

DOJ is pursuing a Secure Encrypted Title 3 (SET3) Public Key Infrastructure (PKI) Prototype, which applies to the Title III Pre-Authorization Approval Sub Process (PAASP). In the first phase, a prototype system has been implemented that will focus on the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). The initial participants are units at FBIHQ and DEAHQ that request, and respond to requests, regarding Title III Electronic Surveillance (ELSUR) records in the PAASP. The prototype will allow DOJ to evaluate operational policies and procedures, and identify communication infrastructure upgrades that may be required to facilitate future inter-component and interagency communication and data sharing.

The mission of both the FBI and DEA is law enforcement, and the implementation of the SET3 PKI is focused on that mission. The SET3 PKI is intended to enhance the confidentiality, authenticity, integrity, availability, and reliability of the current Title III PAASP. It adds the service of *non-repudiation*. It is intended to increase the effectiveness and efficiency of personnel who are in direct support of Special Agent operational personnel.

DOJ has chosen Entrust (Version 4.0) software for the SET3 PKI implementation. Entrust provides the software building blocks for the Certification Authority, Registration Authority functions, and end-user client. The directory will be an X.500 DC Directory v2.2 from Data Connections Ltd. The SET3 PKI will use electronic mail to transfer Title III, ELSUR record check requests between the FBI and DEA. Microsoft Exchange with Outlook has been selected to provide for e-mail. PKI functionality for the Outlook client is provided via the Entrust ready Express snap-in that enables users to sign and encrypt documents. Subscribers will employ the Datakey model 320 smartcard.

The Exchange mail server will maintain an encrypted electronic archive of all ELSUR record check requests and responses. In addition to the built-in transaction log feature of Exchange, an “archive user” account will be set up. All messages sent by any user will go into this “archive user” account as well as to the intended recipient. Only the E-mail system administrator will be able to see or access this “archive user” account. The normal user will be oblivious to the existence of this “archive user.” The archive will be encrypted in a session key which itself is then encrypted in the public key of the intended recipient and, in the Entrust system, in the public key of the sender. All contents of the encrypted archive will be available with either the cooperation of sender or receiver or by administrative key

recovery. Administrative key recovery would not require the cooperation of sender or recipient; the process will be described in the Certification Practice Statement.

Separate from the SET3 PKI pilot, DOJ is pursuing a civil PKI prototype that involves encryption and digital signature support for civil law environment between the DOJ Tax Division and the Internal Revenue Service (IRS). Subscribers from both agencies' headquarters and selected representative field offices will participate in the prototype, as well as DOJ IT support staff. If the initial efforts prove successful, subsequent phases may involve expansion to include additional DOJ components and external agencies (e.g., Executive Office for United States Attorneys (EOUSA)), and Social Security Administration (SSA)).

The civil PKI prototype will install and implement digital signature and encryption capabilities in a limited operational environment, supporting up to 200 participants. This will include secure e-mail and file encryption on the desktop. The system will provide users with authentication, non-repudiation and data integrity. The prototype includes the administration and management of certificates and directories that are needed to provide the security services and support to users. DOJ selected an environment with civil law as opposed to criminal law because of the potential liabilities involved.

The first phase of the civil PKI prototype is being implemented under the direction of the Department's Information Management and Security Staff (IMSS), Information Resources Management, Justice Management Division. A contractor has been selected to provide support for the first phase of activity, primarily through the establishment and operation of a CA at its office in McLean, Virginia.

Each participating agency is responsible for identifying the type of information that will be used in the prototype, and for incorporating such use into the appropriate organization system security plan and other related documentation. In general, the information may involve material protected under the Privacy Act, tax statutes, litigation, or other requirements. All data will be encrypted and signed. Further, litigation data will be transmitted between subscribers and will never be processed by or stored at the CA.

In addition to the efforts cited above, the DEA is proceeding with planning for other PKI pilots. The DEA's Office of Diversion Control regulates the manufacture, distribution, and prescription of controlled substances within the United States. The Office of Diversion Control is seeking to use PKI technology to bring the advantages of e-government and e-commerce to

this regulatory process. DEA envisions using PKI to: (1) permit encryption of communications; (2) replace pen and paper signatures with digital signatures; (3) reduce the amount of paper in processes; (4) speed transaction times; (5) lower costs per transaction; and (6) introduce improved security services to processes, especially important concerning regulatory processes such as pharmaceutical drug (controlled substance) prescription and distribution. DEA expects the above advantages will accrue to all parties to the transaction.

DEA intends to perform a pilot PKI and a Proof of Concept to demonstrate the feasibility of introducing this new technology into the diversion control regulatory process. Such an effort hopefully will demonstrate that the mission critical work of the Office of Diversion Control can be accomplished more effectively and more efficiently; the procedures of the regulatory process can be streamlined to be more convenient for individuals and institutions subject to the regulatory provisions; parties will be able to comply better with the laws and regulations that bear on the areas of privacy, protection of medical records, paperwork reduction, legal liability in connection with prescribing, dispensing, manufacturing and distributing controlled substances, and records management; and forgeries of prescriptions will be substantially reduced. Parties to manufacturing, distributing, prescribing, and dispensing controlled substances will be undeniably accountable for their actions, and liability will be easier to place on the accountable party.

The initial pilot activity is entitled the DEA-Department of Veterans Affairs Pilot PKI (DEA-DVA Pilot). DEA is in the process of completing an Enterprise Requirements Analysis with contractor support, leading up to a Proof of Concept (POC) effort. These efforts will determine the aspects of the relationships between the Practitioner and the Pharmacy that can be enhanced for both parties by the use of a PKI.

The second pilot activity is called the Manufacturing and Distribution Pilot PKI, for which DEA with contractor support is also conducting an Enterprise Requirements Analysis. The requirement analysis will determine the aspects of the relationships between manufacturers, distributors, and pharmacies that can be enhanced for all parties by the use of a PKI. The contractor will deliver a plan to design a POC PKI (the Manufacturers-Distributors POC PKI) to test these enhancements and refine the POC.

11. *National Aeronautics and Space Administration (NASA)*

NASA is currently deploying an agency-wide PKI for a variety of applications that support the agency's mission. Initial uses of PKI include

encrypting and digitally signing e-mail, encryption of files on desktops, and secure web transactions. NASA's Integrated Financial Management Program (IFMP), now in testing, will standardize, across all NASA's Centers, agency business processes ad systems in the areas of: accounting, budget formulation, time and attendance, procurement, travel, asset management, human resources, and grants management. IFMP will make extensive use of NASA's PKI for both encryption and digital signature. NASA expects that numerous other applications and infrastructure components will use PKI capabilities. Near-term candidates include electronic grants, electronic forms, firewalls, and virtual private networks.

NASA has selected Entrust for its CA software, and is running a single CA; a backup CA is under development. Registration Authorities (RAs) will be located at each of the ten NASA Centers and NASA Headquarters. The RAs follow a common set of procedures for registering PKI users (subscribers) and are accredited by an agency team before becoming operational. Over one-half of the Center RAs are operational; the remaining RAs are scheduled to be operational by the third quarter of FY 2000. The CA and RAs are linked via the NASA Wide Area Network.

The NASA PKI must support diverse Headquarters and Center environments, consisting of networked Intel-compatible, Apple and Unix workstations, as well as some standalone workstations in laboratories or special operational environments. The NASA PKI user community is equally diverse, including agency and Center management, scientists and engineers, mission operations personnel, functional staff (e.g., procurement and contracting), information technology specialists, administrative support staff, and other disciplines.

NASA has purchased a license covering the issuance of 24,000 certificates (enough for all of its headquarters and Center employees), and expects all certificates to be fully deployed by the end of 2000.

Subscriber private keys are protected on local hard drives or floppy disks. Each subscriber has two key-pairs, one for signature and a separate one for encryption / decryption. NASA is currently investigating the use of hardware tokens or Smartcards for subscribers. The CA private key is protected by the Chrysalis Luna cryptomodule that is FIPS 140-1 level 2 validated. Data recovery (for encryption keys) is accomplished through functionality provided by the Entrust software.

12. Department of Health and Human Services (HHS)

The Department of Health and Human Services has several PKI efforts underway, most notably those being done by the National Institutes of Health (NIH). NIH has implemented PKI with Microsoft Exchange/Outlook for secure (S/MIME) e-mail. Subscribers are users of NIH e-mail. The project supports both digital signatures and encryption for e-mail, so each user gets two certificates. About 500 certificates have been issued, with plans to expand that to over 15,000 by mid-2001. Certificates are issued using a Microsoft CA server, with registration being effected through the Exchange mail server. Since this application uses software available on desktops and servers, the cost of implementation has been negligible, and substantial savings are expected as paper processes are replaced with S/MIME transactions. Data recovery (for encryption keys) will be accomplished through Microsoft Exchange mail server administration.

Subscriber registration can also occur using the NIH extranet, but only with an extensive paper trail. The core PKI uses a database of user social security numbers maintained by the NIH security office, and a combination of information on the user's Windows NT login and Exchange login. For users with Smartcards, the security office must first identify the user in person before registration consummates. Contractors who go through the registration process must have a government sponsor.

In addition to the work within NIH, HHS is developing an internal PKI to support secure electronic exchange of information among its employees, contractors and others. Further, the Health Care Financing Administration is preparing for implementation of regulations implementing the Healthcare Insurance Portability and Accountability Act governing electronic transmission of medical records and other personal data under Medicare; those regulations call for strong authentication of users and confidentiality of information, requirements which can be met using PKI. Additionally, the Indian Health Service (HIS) is participating in a multi-agency PKI pilot to enable electronic exchange of medical information with Tribal health centers and IHS Clinics. Finally, the Centers for Disease Control and Prevention (CDC) is operating a PKI pilot using VeriSign certificates to exchange morbidity and mortality data with State health departments.

13. Nuclear Regulatory Commission (NRC)

The NRC is currently piloting an Electronic Information Exchange (EIE) program employing PKI in one of its low-level radioactive waste licensing hearings before the Atomic Safety and Licensing Board (ASLB). There are

approximately 10 participants in the pilot representing law firms, state agencies, individuals and government employees. The system uses certificates issued by VeriSign and a webform designed by UWI that provides for digitally signed information transmittal. Documents are digitally signed and then may be transferred using SSL for confidentiality to the NRC EIE server where they are retrieved and downloaded to the NRC's document management system or to an individual desktop. This approach supports the transfer of very large documents and filings that might exceed size restrictions of some e-mail systems. The pilot homepage may be viewed by accessing the NRC homepage www.nrc.gov, then clicking on the EIE located in the toolbar at the bottom.

NRC plans to expand this pilot into a production system to handle all submittals from Nuclear Generating Stations licensees. This would represent approximately 60% of the paperwork submitted to the agency. It is anticipated that this system will be enabled by mid 2000. Participation will be on a voluntary basis. Although licensees will be allowed to submit documents electronically, they will be required, for a short transition period, to submit one paper copy as well as the electronic version. This will still provide some relief to the licensees, as the NRC currently requires as many as 45 to 60 paper copies of some documents submitted in response to regulatory requirements. Late in the summer of 2000 the NRC will issue a rule that will do away with the paper copy requirement and instead allow electronic filing when desired by the submitter.

The EIE system will initially be limited to files no larger than 5 MB using PDF, Word or WordPerfect formats. NRC anticipates that the system requirements will become less restrictive as experience is gained. The webform allows for multiple digital signatures and eventually will be able to encrypt documents that are sensitive in nature. At present, documents requiring encryption (other than SSL session encryption) will not be submitted electronically.

14. *Social Security Administration (SSA)*

SSA has several efforts underway employing public key technology. Each is discussed separately below.

a. SSA has bilateral Social Security agreements with 17 countries that eliminate dual social security coverage and taxes for multinational companies and expatriate workers. In order to qualify for that exemption, employers must complete a country-specific application form for each employee seeking an exemption. Traditionally, these forms have been paper based; however, through its Certificate of Coverage (CoC) Internet pilot, the SSA has

developed and is using a web-based implementation using HTML to create and file e-forms. The web implementation uses SSL for client and server authentication, confidentiality, and integrity. Specifically, the CoC pilot uses the basic security features provided through SSL by establishing a secure pipe for traffic between the client workstations and the SSA server hosting the application. Data is encrypted during transmission only so there are no data/key recovery requirements.

SSA is extending the pilot to give pilot participants the ability to digitally sign and encrypt the CoC e-form. In addition, SSA is migrating to XML in lieu of HTML for web e-forms. Participants may request the XML forms stored on a stand-alone SSA server. The first time retrieval of an e-form will initiate a download of the Internet Forms Viewer plug-in to the client workstation. This viewer software provides participants the ability to complete and digitally sign a CoC request application. The signed request will be encrypted, sent to an SSA stand-alone server, and placed in queue until retrieved by the SSA CoC server. The SSA CoC server will decrypt the form and verify the sender's signature before loading the form, data and signature into the CoC database.

The CoC pilot incorporates several COTS products including UWI.Com InternetForms Designer (to create the electronic forms) and InternetForms Viewer plug in (to view the electronic forms); Internet Explorer and/or Netscape Navigator browser; Netscape Enterprise Web Server (for serving the forms); VeriSign Onsite LRA (to register users in the system); RSA RSARef cryptographic toolkit (to provide cryptographic services on the server side); and Microsoft Crypto API (to provide cryptographic services on the client side).

The CoC clients interact with SSA through the Internet. The client hardware/operating system requirements include an Intel Pentium class PC running a Microsoft 32-bit operating system. The clients are also required to run either an Internet Explorer or a Netscape Navigator browser. A "stand-alone" Netscape Enterprise Web Server serves the electronic forms to the client. The CoC application runs on a UNIX platform under the Solaris operating system. The VeriSign LRA server runs on an Intel Pentium class PC running a Microsoft 32-bit operating system and Netscape server software.

SSA anticipates issuing between 40 and 55 certificates for the CoC pilot. Private keys are encrypted under passwords and stored in software. Most of the SSA customer pilot participants are Human Resource Department staff members from the private sector. The participants are familiar with the use of information technology as a tool but they are not experts in the field of information technology or PKI.

Customers using this system have a pre-existing relationship with SSA. The registration agent uses information from this relationship when approving a certificate request. In addition, pilot participants receive a unique PIN from SSA that is used during the on-line enrollment process. The application's enrollment module is accessed through a secure URL provided to the pilot participants by the registration agent.

This pilot will provide SSA with a controlled test-bed environment in which to develop the architecture requirements necessary to support this and other PKI applications. It will also provide experience in the use, collection and storage of digitally signed e-forms. The pilot will provide valuable insight into SSA's business partners use of PKI technology.

b. SSA also is employing public key technology in their Annual Wage Reporting (AWR) process. AWR is a process where over 6.5 million businesses send their W-2 information to SSA for inclusion in individuals' earnings records. The AWR pilot was conducted to assess customers' perceptions of the utility of two different mechanisms for the submission of AWR files through the use of digital certificates and the Internet. These two mechanisms are Secure Multipurpose Internet Mail Extensions (S/MIME) e-mail, and mutually authenticated Secure Sockets Layer (SSL) sessions. Digital Signature Trust Company (DST) worked with SSA on the pilot.

Over 100 employers participated in the pilot, securely transmitting over 4,000 Annual Wage Reports. Under the SSA/AWR pilot the company representatives applied online for SSA certificates. SSA, acting as its own Local Registration Authority (RA), approved or denied the applications via DST's web-based Local Registration Agent. The approved applicants retrieved their certificates online from DST. Finally, the approved applicants submitted their AWR file as an upload during a mutually authenticated SSL session, or as a digitally signed and encrypted S/MIME email attachment.

The SSA/AWR PKI Pilot used DST *TrustID*™ (X509 v3) certificates for both SSL and S/MIME submissions, and required Netscape and Microsoft browsers with 128-bit domestic encryption or an email client that supports S/MIME. The SSA RAs were each issued a *TrustID*™ certificate on a Datakey Smart Card and accessed the DST LRA application via a mutually authenticated SSL session. DST also provided technical Help Desk services in support of this pilot.

Pilot participants were also asked to share their experiences throughout this process by voluntarily completing three brief online surveys after registration, after certificate retrieval and install, and after submission of their

AWR. Overall response to the pilot was overwhelmingly positive. Sample findings indicated that 100% of respondents would use a process like this again. Seventy-six percent of respondents rated the registration process as easy; only 8% found it difficult. Eighty-three percent of respondents reported that it took them less than two minutes to download and install their certificates. Seventy-three percent of respondents reported that using their digital certificates was easier than they expected. Only 7% found it harder than expected. Finally, 91% said that they found the process easier than how they currently file their W-2s.

SSA intends to allow employers to transmit their AWR file over the Internet in 2001. SSA is evaluating the results of the pilot and exploring whether to implement PKI for all employer based constituents.

15. *Department of Transportation/Federal Aviation Administration (FAA)*

The FAA Flight Standards Service (AFS), the largest of the service organizations underneath the FAA's Office of Regulation and Certifications (AVR), is responsible for the safety of commercial and general aviation in U.S. airspace. AFS inspects and verifies the operation and maintenance condition of aviation aircraft and facilities; sets standards for, conducts test of and certifies the skills of air flight crews operating those aircraft and facilities; and certifies air carrier and agency operations. The AFS safety mission requires that the organization deploys and maintains a significant, geographically dispersed force of Aviation Safety Inspectors (ASI's) in order to meet the high standards of regulation, certification, surveillance, and enforcement for all U.S. commercial and general aviation safety. The Operations Specifications Subsystem (OPSS) is a client server application that has automated the production of air operator Operations Specifications (OpSpecs) documents. OpSpecs are a collection of the regulatory documents by which the FAA governs air operators. This is the application that employs PKI.

Both OPSS and AFS use digital signatures, and more recently, are adopting the use of encryption. Once an OPSS provision is digitally signed and accepted, it is a matter of public record and thus is not encrypted. However, a change proposed by an air operator may be highly sensitive (containing proprietary or competitive information), requiring the use of encryption and hence data recovery for stored encrypted data.

The FAA is using COTS software (Entrust) for the OPSS and AFS PKI, for both digital signatures and encryption. The OpSpec architecture consists of a centralized server located at the FAA accessed through the Internet or

the FAA wide area network. Electronic signature authentication is done through the Internet with a CA server located in Annapolis, Maryland.

The number of individuals currently authorized and proofed for certificates is about 1,000, but that number is growing rapidly to cover all Aircraft Safety Inspectors (over 4,000) as well as over 20,000 users in the industry (over 2000 air operators or agencies with at least ten users of the system per operator / agency). Major U.S. air carriers are participating in this program, with in-person registration services provided by the BTG, Inc., the contractor responsible for the development of OPSSs using COTS software. The number of digitally signed documents is expected to reach many hundreds of thousands.

While the cost savings associated with this effort are difficult to estimate, they are very real. The project decreases the time necessary for an air carrier to have a proposed Operation Specification Paragraph implemented, and therefore cost and safety benefits will be realized. The ability to archive and retrieve digitally signed documents electronically reduces costs associated with managing paper copies. Further, the FAA PKI will interoperate with the Federal Bridge CA thus providing for interoperability with the PKIs of other Federal agencies, leveraging the effort required to issue the digital certificates to FAA staff and contractors.

16. *Department of the Treasury*

The Department of the Treasury has several efforts underway or planned within subordinate elements. These are described separately below.

a. United States Mint: The Mint uses digital signatures and encryption to store and forward file transmission applications. This entails encrypting and digitally signing the data file, then transmitting the file using either File Transfer Protocol (FTP) or other industry standard modem transmission protocols such as zmodem. The data generally comprise marketing demographic information of current or prospective customers of the Mint's numismatic products. The electronic commerce website that the Mint hosts via an ISP (UUNET) uses SSL for its entire sensitive / financial data interaction. The Mint then encrypts and digitally signs the customer orders extracted from the commerce server at the commerce server, then uses FTP to transfer the orders through the internet back to the Mint for processing.

The Mint evaluated PKI products available and certified by the National Security Agency (NSA), and based on the Mint's native enterprise server and networking composition, selected AT&T's Secret Agent.

The Mint is on Treasury / Sprint's public frame relay network. The Mint's field sites (Denver, Philadelphia, West Point, San Francisco, Fort Knox, Customer Care Center) are all connected to the public frame network using full or fractional T1 lines and Treasury mandated Cylink encryption boxes for all links. Access to the Internet is through the frame relay network, then through Treasury's firewalls to the Internet. The PKI end to end logical link is from within the Mint to commercial FTP sites on the Internet.

The Mint's PKI effort is a pilot. Only a handful of certificates have been issued, and slow growth is expected in 2000 to about a dozen certificates as data are gathered on use. Current subscribers range from numismatic product market research firms, to a single Internet SSL commerce focal point which then becomes a Mint internal sender and receiver pair for PKI. As the Mint's procurement division expands into the business electronic commerce area, the Mint expects to use SSL for confidentiality but expects the number of digital signature certificates to increase. Further, as part of the Mint's migration to an Enterprise Resource Planning system, a rapid deployment of new processes ensued including the transmission of sensitive data to entities external to the Mint. To service these needs, the Mint is currently working on an enterprise-wide, all encompassing, security infrastructure redesign, which will incorporate a more robust PKI with digital signatures, secure dialup, and other features.

b. Bureau of Alcohol, Tobacco & Firearms (ATF): Network encryption at the ATF is end-to-end using Cylink Secure Frame units. Digital signatures are used to authenticate one frame unit to another. Specifically, a unique session is created to encrypt the information, using DES encryption. This application uses digital signature to authenticate one frame unit to another and DES encryption on the transmission. There are approximately 250 frame units, each with its own certificate. The private keys are stored within the secure frame unit, which is the subscriber's universe. The frame unit, when initially installed, is registered with the administration server.

Digital signatures are also used to authenticate users to create a protected dial-in session with the ATF network. This enables agents, inspectors and managers who are on the road to communicate. It has also permitted work-at-home in the event of illness. This capability is provided by the Cylink SecureAccess system, which includes a SecureGate server that functions as a Certification Authority. The client has Secure Traveler software, which communicates with the SecureGate server. Once logged into the ATF network, dialup users can access ATF applications, ATF's Intraweb, the Internet, and the Treasury Enforcement Communications Systems. Almost 2,300 certificates have been issued to ATF employees and contractors for this application. Private keys are stored on the client workstation.

The user backs up encryption keys to a diskette in case of hardware failure. Registration is performed using ATF's standard information systems access form, with the supervisor or contracting officer's technical representative signing the form. The total cost to stand up this system was $500,000.

c. United States Secret Service (USSS): The USSS plans to implement a PKI to ensure the identity and the integrity of the user and the system they access.

The pilot program employs Entrust software. The operating environment in which the PKI will be deployed is offline. Mission critical information will be extracted from enterprise files and downloaded onto CDs for distribution to the field. The field offices that will be receiving these CDs have been previously identified. These offices will be the subscribers (users) of the certificates; 150 certificates are expected to be issued. The certificates will be used to authenticate subscribers to the CDs. The private keys will be protected through the traditional user name and password combination. The registration process of certificates for the pilot program is non-standard, in that the Certification Authority (CA) will initiate the certificate application. Upon successful completion of the Subscriber's identification and authentication process, the CA shall create a certificate and notify the Office Security Representative, and make the certificate available to the field office.

Beyond this pilot, additional USSS PKI efforts are planned. The exact requirements, while still evolving, are specific enough to allow for the development of security policies and the identification of target applications.

d. Bureau of the Public Debt (BPD): The Special Purpose Securities System (SPSS) of the Bureau of the Public Debt processes a wide variety of state, local and other financial securities (State and Local Government Series (SLGS) Time and Demand Deposit securities, Domestic Series (Refcorp) Time and Demand Deposit securities, Tax and Loss securities and 5% Rural Electrification Administration (REA) securities). SPSS processing includes issuance, account maintenance, payments and reporting.

The existing backend application employs Power Builder 5.0 and uses mainframe DB2 and Microsoft SQL-server database architectures. In early December 1999, the Bureau implemented a new approach that provides an interface via the Internet for SLGS trustee financial institutions. This interface allows these business partners to submit SLGS subscriptions and to make account inquiries. By mid-2000, the SPSS system will provide an interface with other Federal agencies such as Treasury's Financial Management Service and the Federal Reserve Bank in Richmond. The authentication needs for this approach are being met by a PKI, using software

supplied by Entrust. The operating environment was developed under Information System Life Cycle (ISLC) guidelines, using Client/Server architecture. The operating system is Microsoft NT. The majority of SPSS database tables reside on Microsoft SQL-Server with some SPSS database tables residing in DB2 on the Bureau OS/390 mainframe.

BPD issued the first 50 certificates in December 1999, and we expect these numbers to grow to approximately 500 by Summer 2000. Private keys will reside in password protected client software. The subscribers are state and local government trustee financial institutions. A designated customer authority serves as the Registration Authority (RA), and is responsible for (a) verifying that a requester has a valid reason to have a digital certificate; and if so, (b) following an established procedure for requesting the certificate from BPD. The request is reviewed and, if approved, the certificate is issued and a PIN mailed to the RA, which sends it to the requester. The requester goes to the web site and uses the PIN to retrieve the certificate and subsequently access the application

Public Debt expects additional business uses of its PKI to be implemented in calendar year 2000 to include applications shared by both the Treasury and the Federal Reserve System. Two application pilots are currently in testing.

17. *Department of State (DOS)*

The Department of State is embarking on a PKI initiative in order to support worldwide secure communication among DOS personnel in the U.S. and abroad at over 200 posts. It is paramount to the security of government personnel and to the global interest of the U.S. that DOS personnel be able to carry out communications securely in an expeditious manner among themselves, with other agencies of the U.S. Government, with other Governments, with U.S. citizens here and abroad, and with foreign nationals. Many times, in order to protect U.S. citizens and U.S. interests, these communications may have to be deciphered even if the intended DOS recipient is not available. Encryption key recovery technology will be used for this purpose under three scenarios: (a) the affected individual may need key recovery (sometimes referred to as self-recovery) due to a variety of reasons including loss of password, or corruption of key or token; (b) the affected organization may require key recovery in case the individual is inaccessible (e.g., on extended leave, on travel, death, disability, or employment termination); and (c) law enforcement organizations may need access to the keys or need the plaintext in order to decipher lawfully obtained (e.g., through subpoena, or court authorized wiretap) ciphertext.

In addition to these elements, the DOS has another requirement: the potential need to abandon an embassy or a post and destroy cryptographic equipment or render all equipment useless by zeroizing the cryptographic keys. If that happens, DOS may later need to reconstitute the cryptographic context, possibly expeditiously. Doing so may also require using commercial communications infrastructure available in other countries, with no guarantee of security. Re-establishing the cryptographic context may entail simply recovering current (old) decryption private keys and / or creating and registering new key management key pairs.

Another DOS requirement is that the key recovery scheme should be able to support decryption of incoming encrypted communication as well as outgoing encrypted communication. DOS employs many foreign nationals who use DOS IT resources. If one of these foreign nationals were a target of investigation, it would be desirable to decrypt the outgoing encrypted communication originated by the target of investigation.

With these needs in mind, DOS is participating in a PKI e-mail pilot with the National Security Agency (NSA). The objective of the pilot is to explore the ability of commercial products to support the DOD Class 4 (High Assurance) PKI. Under this pilot, DOS will begin issuing certificates to its employees and contractors in early 2000. Private keys will be held on Datakey smart cards. The commercial PKI provider is General Dynamics using the Cybertrust PKI product suite. The initial PKI enabled application will be secure e-mail over the Internet, with both digital signature and encryption capabilities (separate certificates for each function).

The Cybertrust product supports key recovery using key escrow. The LRA is responsible for generating the subscriber's encryption key-pair. The key management algorithm is RSA. The LRA is operated under two-person control. The RSA private key management key is encrypted using a random triple-DES key and the wrapped key is stored at the LRA workstation. The triple-DES key is double encrypted using each LRA operator's public key. This wrapped token is also stored at the LRA workstation. Thus, both LRA operators need to be present to unwrap the triple-DES key and then to unwrap the private key management key.

18. *U.S. International Trade Commission (USITC)*

USITC hopes to implement PKI as a general "network service" that would be used for all sensitive authentication situations, not just a single application. However, the most important applications for the justification and budget process are related to USITC's quasi-judicial role in administration of import-injury investigations. This would cover electronic filing of attor-

ney briefs, electronic document service (distribution of documents to all parties in a case), and probably on-line completion of questionnaires sent to parties. Internally, USITC wants to implement single sign-on to all applications via an "authentication server" which might use PKI as a front end to a symmetric key system like Kerberos. Thus, USITC's subscriber base for certificates is expected to number at least 500 and will include internal staff, attorneys and paralegal staff at law firms participating in cases before the agency, business people (accountants, company officers, attorneys) at firms involved in cases (fill out USITC questionnaires), personnel at Federal courts that review USITC determinations (Court of International Trade, etc.), and other Federal consumers of USITC work (e.g., U.S. Trade Representative).

USITC is redesigning its network architecture, focusing on open-standards based products as much as possible (IMAP, TCP/IP, HTTP, LDAP, PKI, SQL, and XML.) For server operating systems, USITC expects to have both UNIX (Sun, Linux) and Microsoft NT; for clients, USITC expects to continue to use the "consumer" version of Windows, but with an emphasis on making all applications web-based to maximize portability/flexibility and minimize desk-side maintenance. USITC is considering a Java/EJB component framework for applications, but will no doubt acquire applications based on COM/DCOM.

USITC expects that the use of PKI will result in benefits associated with: (1) lower costs compared to paper distribution (USPS mail, FedEx); (2) faster questionnaire processing with fewer errors; (3) lower public paperwork burden; (4) lower internal computer admin costs via single-sign-on; (5) improved security; and (6) compliance with the Government Paperwork Elimination Act.

19. *Department of Veterans Affairs (VA)*

VA has embarked upon a significant effort to use PKI in a wide variety of applications. The VA PKI Project, which began in 1999, provides enterprise-wide policy and a shared infrastructure for all VA applications that require PKI services, including authentication, integrity, non-repudiation and confidentiality. This project has Department-wide support and funding. Project efforts to date have focused on gaining an understanding of the technology and standards, policy development, and establishing an initial capability that can evolve over time as the demand for PKI increases and the technology matures.

VA has an infrastructure in place that supports several ongoing pilots and will expand to accommodate production use by employees, veterans, and

external business partners. A certificate policy, published on the VA PKI website (http://www.va.gov/vapki.htm), provides the cornerstone for trust and interoperability within the Department and with outside partners like DOD, SSA and DOJ. The current infrastructure uses VeriSign as the CA, in combination with PKI-enabled Microsoft e-mail and browser clients at the desktop. Approximately 1000 certificates have been acquired for use with the pilots. Certificates are downloaded to workstation certificate stores; users are required to enter a password each time they digitally sign or decrypt information. At present, registration is controlled centrally. VA has contracted with CygnaCom Solutions for help desk, management support, and development of procedures and a database for distributed registration.

VA is currently upgrading to VeriSign's enterprise version, which has a number of enhancements to facilitate Department-wide roll out. These include encryption key recovery, locally hosted enrollment, and integration of certificates with Microsoft Exchange's global address list. Contractor support expenditures for initial pilot infrastructure amount to approximately $600,000 so far. Significantly greater investment will be required in the future to expand the user base beyond the initial pilots and to PKI-enable applications. This investment falls within VA's overall strategy to enhance its information security posture through strong centralized policy and management and enterprise-wide infrastructure capability.

VA's electronic form demonstration, at https://www.va.gov/sec/vha/FormsDemo/, shows how the public to file forms electronically can use PKI in combination with electronic form software. This demonstration uses PKI for authentication, data integrity, digital signature, access control and session encryption through SSL. It uses VeriSign's On Site service along with a COTS forms software package. The form that VA selected for demonstration purposes is a VA Form 22-1999, a Veterans Benefits Administration form used by school administrators and VA benefits staff for confirming student attendance at a school. In addition to making the electronic version of the form available to obtain information directly from the member of the public, this demonstration includes the digital signing of both the form, the form logic and the data contents. After the form is digitally signed, no entry can be altered. When the form is then submitted, it is captured in a database and data are extracted from it. The original signer may retrieve the signed form from the database. The data from the form can be copied into a new copy and updated with current information to save time for the user. This new, updated form can then be signed, and submitted as a new entry to the database.

VA student enrollment certificate representatives at nine schools were designated to participate in the Access America for Students pilot beginning

in September of 1999. Participants in this initial pilot were provided the capability to enroll for VA digital certificates and use these certificates with the VA Forms Demonstration in order to become familiar with PKI use. The VANetCert application will move VA's enrollment certification form to the Internet in early 2000. For this application, PKI offers strong authentication and digital signature capability.

VA NetCert is one of three electronic service delivery applications under development for benefits processing now considering use of PKI for digital signature and strong authentication. VA NetCert will provide educational institutions the ability to electronically submit student enrollment information to VA. VONAPP (VA on-line Application) will provide a web portal for filing original applications for VA education, compensation, pension, and vocational rehabilitation and employment benefits. Students receiving VA education to electronically verify their enrollment every month over the Internet will use WAVE (Web Automated Verification of Enrollment). PKI digital signature and stronger authentication capability will set the stage for fully electronic processing for all but the most complex transactions. GSA's ACES contract is a potential source of supply for veterans' digital certificates, and for assistance in PKI enabling these applications. VA is also helping to steer the ACES contract through its participation as a charter member in the ACES Customer Advisory Board.

Separate from these efforts, DEA and VA are working together to evaluate the effectiveness of strong technical controls, like PKI, to improve the security of electronic prescription orders. At present, physicians and pharmacists in many states already use Electronic Data Interchange (EDI) technology to transmit prescriptions for non-controlled substances. However, current DEA regulations do not permit use of this technology for controlled substances. DEA is working with Performance Engineering Corporation (PEC) to develop the design for a pilot PKI based electronic prescription system for controlled substances that will be tested in a VA hospital environment. A number of alternatives are under consideration for protecting private keys – including software based storage and hardware based storage (e.g. smart cards). After evaluating the results of the pilot, the DEA will develop and release revised regulations to allow for the electronic transmission of prescriptions for controlled substances. Ultimately pilot results could have broad applicability. Over 850,000 practitioners are currently registered with the DEA to prescribe controlled substances. Pharmacists may also be involved because of their record keeping requirements.

VA's security, general counsel, inspector general and law enforcement communities have an immediate need for secure communication channels to convey highly sensitive information, e.g., concerning investigations or litigation in progress, discovery of system vulnerabilities, information

security incident reporting and response, and management of user accounts. These communities need to be able to communicate securely within the Department and outside via the Internet. Without the assurance of confidentiality that encryption provides, electronic communication is often not an option. VHA's Medical Information Security staff (MISS) and members of the Department's information security work group are actively participating in the secure e-mail test, as a prelude to providing this capability to field station advisory group members, and ultimately, information security officers. Information security officers will require training to perform their dual role - as local certificate registration authorities and PKI end users.

VA has contracted with Cygnacom Solutions Inc. to develop a distributed proofing procedure and database application to support the field IS-security officer role in digital certificate identity proofing, registration and associated record keeping requirements. PKI will be used for authentication, integrity, digital signature and encrypting the sessions. Only authorized, PKI authenticated users will be able to access this database application. The application is currently in the testing phase. The information security officer community who will access this application, when fully deployed, will number approximately 250.

Other VA PKI pilots currently in the planning stage are an inspector general limited access database, a VHA credentialing application, and secure mechanisms for exchanging sensitive information with SSA concerning medical evidence to support SSA disability adjudications.

AGENCY	PRODUCT OR COMPANIES USED	S/MIME	DIGITAL SIGNATURE	CERTS ISSUED (IF INDICATED)	PLANNED EVENTS
National Finance Center	Entrust		YES	400	PKI based access to employee payroll records
Bureau of Labor Statistics	VeriSign, Microsoft Browser, Netscape Browser		YES		To support applications beyond data collection utilizing PKI
National Institute of Standards and Technology	Entrust, Windows NT, Eudora V3	YES		3000	Re-engineering business processes to incorporate PKI
U.S. Patent and Trademark Office	Entrust		YES	>570	By Feb 2001, USPTO expects to migrate to production use; up to 10,000 certificates
Department of Defense (military departments covered separately below)	Eudora Cygnacom Motorola Entrust Spyrus J.G. Van Dyke Booz-Allen Hamilton	YES		2000	Consideration of smartcard to hold PKI credentials
Department of the Army	Microsoft Outlook	YES		1200	By 2001 goal is issuance of 20,000 certificates
Department of the Navy	Netscape suite, Microsoft suite, Apache SSL, Lotus Domino V.5, Qualcom, Eudora, Lotus Notes, KyberPass	YES	YES	2000	Consideration of SmartCard to all personnel for authentication
Department of the Air Force	Microsoft Outlook	YES			Automated business services
Department of Energy	Entrust, Cygnacom, Microsoft Exchange, PeopleSoft	YES		2000	Pilot with Travel Manager for requests and claims using PKI

AGENCY	PRODUCT OR COMPANIES USED	S/MIME	DIGITAL SIGNATURE	CERTS ISSUED (IF INDICATED)	PLANNED EVENTS
Environmental Protection Agency	E-Lock Tech, Assured Transaction (ATS V.2.1), Adobe Acrobat GemSafe Smartcards, Netscape Navigator	YES	YES	50	Business and to employee payroll records regulatory processes are to be enabled using PKI
Federal Deposit Insurance Corporation	Entrust V.3.0 ICL X.500 V.7 Microsoft Outlook		YES	2000	Migrating all core PKI users to Smart Cards and Building badges
General Services Administration	Entrust CA & Toolkit, NDS AccessGear Smartcards		YES	ACES	
Department of Justice	Entrust V.4.0		YES		
National Aeronautics and Space Administration	Entrust, Chrysalis Luna, Cryptomodule	YES	YES	1,000	Plan is to issue 24,000 during 2000 to cover wide range of internal and external business processes
National Institutes of Health	Microsoft Exchange-Outlook	YES		500	Use to support transactions with trading partners
Nuclear Regulatory Commission	VeriSign, UWI Webform		YES	YES	Use to support transactions with licensees
Social Security Administration	VeriSign, UWI.COM IntelForms Designer, Microsoft Crypto API		YES	55	Plan is to apply PKI to wide range of business applications involving trading partners
Federal Aviation Administration	Entrust, AFS PKI		YES	4000	Major Air are participating; plan to issuel over 20,000 certificates for Carriers aircraft operational documentation
United States Mint	SSL (UUNET), AT&T's Secret Agent, Cylink		YES		Re-design of security infrastructure underway which will incorporate PKI

AGENCY	PRODUCT OR COMPANIES USED	S/MIME	DIGITAL SIGNATURE	CERTS ISSUED (IF INDICATED)	PLANNED EVENTS
Bureau of Alcohol, Tobacco and Firearms	Cylink Secure Access System, SecureGate, Secure Traveler		YES	2300	
U.S. Secret Service	Entrust			150	Evolving security policies and target application for PKI
Bureau of the Public Debt	Power Builder 5.0, SQL-Server Architecture, Entrust, Microsoft NT			50	Approximately 5000 certificates will be issued during 2000 to support transactions with trading partners
Department of State	CyberTrust PKI product suite, DataKey Smartcards, PKI-Email pilot with NSA	YES	YES		
U.S. International Trade Commission	Kerberos, IMAP, TCP/IP,HTTP, LDAP, SQL & XML Architecture, UNIX (SUN,Linux), Microsoft NT, Java/EJB, VeriSign	YES		500	
Department of Veterans Affairs	CygnaCom, VeriSign, Microsoft Exchange Global Address List, EDI Technology, Smartcards	YES		1000	Secure information project allowing transfer with SSA using PKI

Appendix B: Charter of the Federal Public Key Infrastructure Policy Authority

1. Background and Purpose

1.1 The Federal Public Key Infrastructure Policy Authority (Policy Authority) sets policy governing operation of the Federal Bridge Certification Authority (FBCA), to provide a mechanism for agencies employing public key technology to interoperate efficiently. The FBCA allows an agency's Public Key Infrastructure (PKI) to trust digital certificates issued by other agency PKIs. The Policy Authority is created under the Federal CIO Council (Enterprise Interoperability and Emerging Information Technology Committee) and pursuant to Federal CIO Council authority.

1.2 The Policy Authority comprises agencies who wish to interoperate their PKIs in an efficient fashion. Membership is voluntary. Determinations by the Policy Authority apply to the issuance of certificates by member agencies but do not prescribe how those agencies are to rely on the certificates for transactions; agencies are free to accept or reject certificates issued by other agencies at their discretion, using Policy Authority determinations to assist in making informed decisions.

1.3 The Policy Authority makes no guarantees against fraud or loss resulting from its activities.

2. Roles and Responsibilities of the Policy Authority

2.1 Approving the FBCA Certificate Policy and Certification Practice Statement.

2.2 Entering into a voluntary agreement with the FBCA Operational Authority (FBCA OA) which establishes that: (a) the FBCA OA will effect or terminate interoperation with Federal agencies only when directed by the Policy Authority; (b) the Policy Authority may review FBCA OA activities for compliance with the FBCA Certificate Policy and Certification Practice Statement; and (c) either party may unilaterally terminate the agreement after appropriate notice to the other party.

2.3 Coordinating legal, policy, technical and business issues related to agency PKI interoperability;

2.4 Performing liaison efforts with external parties, including companies, state and local governments, and foreign governments. The Policy Authority covers only U.S. Federal agencies and the FBCA initially will support interoperation only among Federal agency PKIs; ultimately, interoperation through the FBCA will be extended to parties external to the Federal government, when and how the Policy Authority deems appropriate.

3. Membership and Organization

3.1 Membership in the Policy Authority is divided into two categories: observer and voting.

3.1.1 Observer membership is automatic and is granted to any agency wishing to participate. Each agency may have multiple observer representatives. Except as provided in Section 3.1.3 below, all agencies who are members of the Federal PKI Steering Committee shall be considered observer members of the Policy Authority.

3.1.2 Voting membership (one vote) is granted to an agency when that agency applies for interoperation with the FBCA and is accepted by the Policy Authority for that purpose. Where the applicant is subordinate either to a Cabinet-level department or an independent entity of comparable stature as set forth in Section 8 below, voting membership (one vote) shall be vested in the superior organization. Voting membership terminates if the agency's interoperation with the FBCA is terminated for any reason.

3.1.3 The following agencies shall have permanent voting membership (one vote each): Office of Management and Budget, Department of Justice, General Services Administration, Department of the Treasury, Department of Defense, and Department of Commerce. Each agency listed above shall not vote upon its own application for interoperation with the FBCA.

3.2 The Policy Authority may have subordinate committees or working groups as determined by majority vote of the voting membership, to support its operation.

4. Officers

4.1 The Policy Authority shall have a Chair and a Vice Chair, both selected by majority vote of the voting membership and approved by the Chair of the Enterprise Interoperability and Emerging Information Technology Committee. The Chair shall serve a two year term. The first Vice Chair shall serve a one year term, and subsequent Vice Chairs shall serve two year terms, thus providing overlap with the term of the Chair.

4.2 The Policy Authority shall have a Secretary appointed by the Chair who shall record minutes of all Policy Authority meetings and be responsible for administrative matters.

5. Operation

5.1 Meetings shall be held on a schedule to be determined by majority vote of the voting and observer membership, with each agency having one vote per Section 8.1 below. The Chair or, in his or her absence, the Vice Chair, shall preside. All members will be given reasonable notification before any vote is called, all votes shall be recorded, and the results of voting will be published.

5.2 For actions requiring votes, the voting may be done at a Policy Authority meeting, through remote means, or by proxy granted by the

member agency to another member agency or to the Chair. Each voting and, where applicable, observer member agency shall be required to cast a vote, except when recusal is necessary owing to a conflict of interest. Failure of a voting or observer member to vote during the voting period will be considered as a proxy given to the Chair.

6. Application for Interoperation with the FBCA

6.1 The Policy Authority shall develop a procedure to be used by agencies wishing to apply for interoperation with the FBCA. The procedure shall be approved by majority vote of all voting members and shall cover: (a) how the applicant agency proposes to map its CA Certificate Policy to the FBCA Certificate Policy respecting certificate levels of assurance; and (b) what duties the applicant agency will have if it is accepted for interoperability with the FBCA, expressed in the form of a Memorandum of Agreement (MOA) between the Policy Authority and the applicant agency.

6.2. Upon receipt of an application, the Policy Authority shall review the application and make a determination whether to accept it as received, accept it with changes (such as a different policy mapping than the applicant proposes), or reject it. This determination shall require at least 75% majority vote of the voting membership (excluding any agency which must recuse itself as set forth in Section 3.1.3 or 6.3). Review of the application preparatory to such a vote may be assigned to a committee or working group of the Policy Authority. All members (voting and observer) shall be afforded an opportunity to review the application and make their views known to the voting membership prior to the vote being taken. Members who oppose accepting the application shall be given a full opportunity to have their concerns heard and discussed.

6.2.1 If the application is accepted without changes, the applicant agency and the Chair of the Policy Authority shall sign the MOA, and then the Chair shall instruct the FBCA Operational Authority, in writing, to take action to effect interoperability between the applicant agency and the FBCA.

6.2.2 If the application is accepted but with changes required by the Policy Authority, the applicant agency will be apprised, and if they agree with the changes, the process in 6.2.1 shall be followed.

6.2.3 If the application is rejected, the Policy Authority shall apprise the applicant agency of the reasons for the rejection. The applicant agency may then revise its application and reapply without prejudice.

6.3 If, subsequent to approval for interoperability, an agency is found to be or admits that it is in material noncompliance with the MOA, the Policy Authority by at least 75% majority vote of the voting membership (excluding the agency in question) shall determine what action to take, which may include termination of interoperability but not expulsion from

the Policy Authority or any action contrary to this charter. The agency in question shall have a full opportunity to participate in these deliberations, but shall not cast any votes. The Policy Authority shall develop procedures approved by majority vote of the voting membership describing how it will perform this function. At their discretion, member agencies may cease or restrict interoperability with the affected agency prior to this determination.

7. Revisions to Charter

7.1 Revisions to this charter may be made upon at least 75% majority vote of the voting and observer membership, with each agency having one vote per Section 8.1 below.

8. Nomenclature

8.1 "Agency" shall mean any executive agency as defined in 5 U.S.C. § 105. It shall include independent executive departments, but not subordinate elements within an agency.

8.2 "Representative" shall mean the person chosen by the agency to attend the meetings of the Policy Authority as a voting or observer participant.

8.3 "Voting member" shall mean any agency that has been determined to be eligible to vote on matters as set forth in Section 3.1.

8.4 "Observer member" shall mean any agency that has not been determined to be eligible to vote on matters as set forth in Section 3.1, but may vote on other matters set forth elsewhere in the Charter.