GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 10, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Subject: *Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities*

This letter is in response to your request that we examine our advice to executive branch agencies regarding commercial managed service public key infrastructure (PKI) solutions to see if the advice is consistent with current federal policy and private sector best practices. Specifically, over the past several years, staff from various agencies has asked for informal advice on these matters. Our informal advice was based on the control environment described to us by the agencies. This control environment, which is discussed later in this letter, resulted in the informal advice that the agencies may incur a greater burden in ensuring that a contract certification authority whose certificates are used in financial management applications[1] has implemented an adequate system of internal controls than would be necessary if the certification authority were implemented internally. However, if agencies are willing to accept this potential increased burden by accepting and mitigating the potential risks (not all of which may be known and understood at this time) associated with commercial certification authorities contracting out, a certification authority may be able to provide the same level of security assurances as an internal certification authority. One key aspect of mitigating the risk will be the close involvement of agency personnel in the commercial implementation. We also told the agencies that until we were formally requested by an agency to review a commercial service provider's system, we could not express a formal position. To date, we have not received such a request.

We recognize that PKI services can be used to help mitigate the significant risks present in the federal information technology (IT) systems that have led GAO to

[1] Financial management systems include financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. Financial systems are composed of one or more applications that are used for (1) collecting, processing, maintaining, transmitting, or reporting data about financial events; (2) supporting financial planning or budgeting activities; (3) accumulating and reporting cost information; or (4) supporting the preparation of financial statements. Mixed systems support both financial and nonfinancial functions of the federal government or components thereof. (Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, div. A., § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sept. 30, 1996)).

conclude that information technology security is a high-risk area.[2] Although PKI systems can help mitigate some of these risks, GAO and the executive branch have recognized that implementing an effective PKI solution is complex and the internal control techniques selected are a critical component of successful efforts. Accordingly, when agencies have requested our views on commercial managed service PKI systems, we have responded by providing the characteristics of good systems and examples of the types of controls we would expect to see should we audit such systems, regardless of whether they are operated by the agency or a contractor. This advice was grounded in our experience with electronic signature systems used in financial management systems and GAO's general internal control standards work under 31 U.S.C. § 3511. For this particular subject, we also used control objectives and security requirements generally outlined in executive branch documents such as Office of Management and Budget (OMB) Circular A-130, applicable National Institute of Standards and Technology (NIST) standards and guidance, the General Services Administration's (GSA) Federal Bridge Certification Authority's practices statement, and guidance on electronic records provided by the Department of Justice. The guidance contained in these documents is consistent with the internal controls discussed in this report.

One purpose of a PKI is to generate electronic signatures. In our evaluation of electronic signature systems, GAO has adopted criteria that are technology neutral. Similarly, the examples discussed in this letter of the types of risks that agencies need to consider in their efforts to implement a critical component of a PKI—the certification authority—and the examples of control objectives that can be used to help understand whether the control techniques selected are adequate to mitigate those risks generally apply to certification authorities regardless of whether they are operated by a commercial provider or the federal agency.

Background

While we have performed several studies looking at OMB's leadership in the electronic signature areas at the request of congressional committees, we have not conducted a survey of private sector best practices in the PKI area.[3] As you know, the Government Paperwork Elimination Act (GPEA) authorized OMB to develop procedures for the use and acceptance of electronic signatures by executive agencies.[4] The act required that OMB develop those procedures in a manner that is "compatible with standards and technology for electronic signatures that are

[2] U. S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

[3] See U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: February 26, 2001), and U.S. General Accounting Office, *Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies*, GAO-04-157 (Washington, D.C.: December 15, 2003). Although GAO has not issued a best practices guide that applies to certification authorities, GAO has issued several guides to help agencies understand information technology risks and evaluate their systems. For example, see U.S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations—A Supplement to GAO's May 1998 Executive Guide on Information Security Management*, GAO/AIMD-00-33 (Washington, D.C.: November 1999), *Federal Information System Controls Audit Manual: Volume I Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999), and *Executive Guide: Information Security Management—Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[4] Public Law 105-277, § 1703 (1998).

generally used in commerce and industry and by State governments."[5] To this end, OMB is required to consult with private sector bodies and state entities that set standards for the use and acceptance of electronic signatures. Although OMB has developed this guidance, it does not specifically address the controls that are needed for certification authorities. Thus, when we respond to an agency's request for informal advice on a proposed PKI solution, we are not attempting to create policy regarding PKI solutions, but are giving our views on what we would consider an adequate internal control structure to address the risks associated with such systems based on the standards that we would follow when conducting an audit under our general audit authority using standards developed pursuant to our authority under 31 U.S.C. § 3511 and relevant executive branch guidance. If we found that a particular system's internal controls were inadequate, or that the executive branch guidance was insufficient to adequately protect a PKI system, our report would include recommendations to improve the internal control environment.

As for any set of internal controls, our views on whether commercial managed services for hosting PKI solutions are appropriate for certain federal agency needs are not static but depend on the application, level of risks, costs, and other factors, as required by numerous statutes. We generally recommend that a critical component of a PKI, the certification authority, remain under federal agency control when that certification authority is used in substantial financial management transactions. This position is based on the internal control structure, as described to us by the agencies, used by commercial certification authorities. Accordingly, the agencies may incur a greater burden in ensuring that a contract certification authority has implemented an adequate system of internal controls than would be necessary if the certification authority were implemented internally. However, if agencies are willing to accept this potential increased burden—which will require close involvement of agency personnel in the commercial implementation—contracting out a certification authority may be able to provide the same level of security assurances as an internal certification authority.[6] We do not believe that there is any theoretical reason why a commercially provided certification authority cannot provide the same level of assurance as one maintained within a federal agency. The Department of Justice has issued guidelines that can help an agency understand the legal risks associated with contracting out data management and storage functions.

This letter also discusses some of the internal control risks associated with a certification authority that issues certificates that are used as evidence of an agency's intent to be bound to financial management transactions and some of the internal control objectives that are needed for such a certification authority regardless of whether it is hosted by a federal agency or a contractor. It also discusses agency use of certificates issued by commercial activities for financial management applications.

[5] Id. at 1703(b)(1)(A).

[6] The exact process that should be used to obtain a contractor for these services is beyond the scope of this letter. However, the acquisition process should, at a minimum, conform to the requirements contained in the Competition in Contracting Act of 1984 (41 U.S.C. § 253, *et seq.*) for civilian agencies and the National Defense Authorization Act for Fiscal Year 2003 (10 U.S.C. § 2304, *et seq.*) for defense agencies.

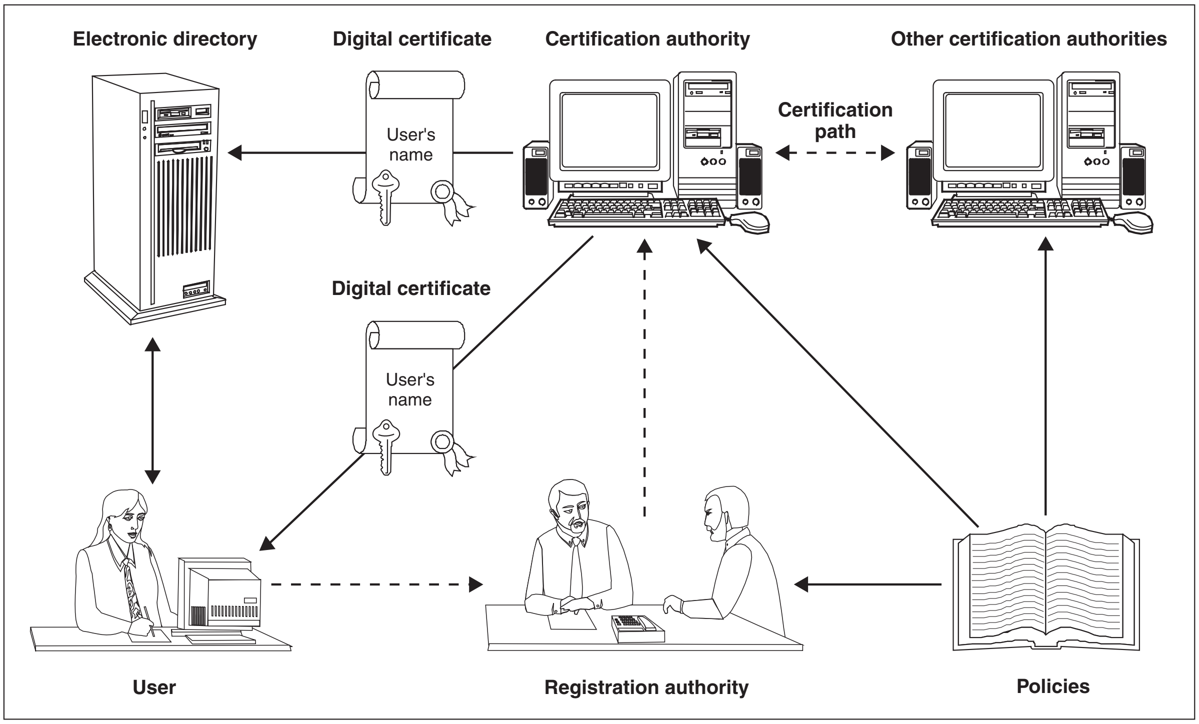
Digital Certificates and Certification Authorities Link Public Keys with Specific Users to Convey Trust

A PKI is a system of hardware, software, policies, and people that can provide a range of security assurances including authentication, data integrity, data confidentiality, and nonrepudiation. PKIs provide a desired level of trust using public key-based cryptographic techniques to generate and manage electronic "certificates."[7] These certificates are used to link an individual or other entity to a public key that can be used to validate the information provided by the entity or individual or facilitate data encryption. Specifically, these certificates are used to verify digital signatures (providing authentication and data integrity) and facilitate data encryption (providing confidentiality). A properly designed and implemented PKI can also be used to ensure that a given digital signature is still properly linked to the individual or entity associated with it (providing nonrepudiation). A properly designed and implemented PKI can satisfy the criteria we use to evaluate systems that produce electronic signatures.

In a small community where everyone knows everyone else, users can individually give their public keys to the people with whom they wish to deal. In a large-scale implementation, where it is necessary for individuals or entities that may not know each other to conduct transactions, it is impractical and unrealistic to expect that each user will have previously established relationships with all of the other potential users in order to obtain their public keys. One way around this problem is for all PKI users and relying entities to agree to trust a third party who is known to everyone. The basic technical components for achieving third-party trust include (1) digital certificates, which link an individual to that user's public key; (2) certification authorities, which create these certificates and vouch for their validity to the entities relying on the PKI; (3) registration authorities, which are in charge of verifying user identities so that the appropriate key pairs and digital certificates can be created; and (4) certification paths, which are used for recognizing and trusting digital certificates issued by other PKIs in order to create larger, connected networks of trust. In addition, a set of written policies establishes the security assurances that an organization needs to achieve and the practices and procedures that will be followed to achieve and maintain those assurances. Figure 1 shows the various components of a PKI, each of which will be discussed in more detail.

[7] Additional information on public key cryptography and PKI issues can be found in our report on challenges associated with implementing PKI technologies. U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: February 26, 2001).

Figure 1: Basic Components of A PKI



Sources: GAO. Copyright © Corel Corp. All rights reserved, Art Explosion.

Certificates and Certification Authorities Are the Technical Mechanisms for Conveying Trust in a PKI

A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity.[8] It is created by placing the entity's name, the entity's public key, and certain other identifying information in a small electronic document that is stored in a directory or other database. Directories may be publicly available repositories kept on servers that act like telephone books for users to look up others' public keys. The digital certificate itself is created by a trusted third party called a certification authority, which digitally signs the certificate, thus providing assurance that the public key contained in the certificate does indeed belong to the individual named in the certificate. A certification authority is responsible for managing digital certificates. The purpose of the certification authority is to oversee the generation, distribution, renewal, revocation, and suspension of digital certificates. The certification authority may set restrictions on a certificate, such as the starting date for which the certificate is valid as well as its expiration date. It is at times necessary to revoke digital certificates before their established expiration dates, for example, when the certificate holder leaves the issuing organization or when the private key is compromised. Therefore, the certification authority is also

[8] Certificates can be issued to computer equipment and processes as well as to individuals. For example, companies that do a lot of business over the Internet obtain digital certificates for their computer servers. These certificates are used to authenticate the servers to potential customers, who can then rely on the servers to support the secure exchange of encrypted information, such as passwords and credit card numbers.

responsible for providing certificate status information and may publish a certificate revocation list in a directory or maintain an online status-checking mechanism. The PKI software in the user's computer can verify that the certificate is valid by first verifying that the certificate has not expired and then by assuring that it has not been revoked or suspended.

Before the certification authority can issue a certificate to a user, it must verify the user's identity in accordance with the organization's preset policies. In some cases, the certification authority is set up to perform the identification and authentication of users by itself, but often this function is delegated to separate entities called registration authorities. A user's identity is verified through one of two means, based on the level of security that is deemed necessary by the organization. In the first method, the user would need to appear in person at the registration authority and present identity documents such as a birth certificate or passport. A second, less secure method, involves the confirmation of a shared secret through an online application. For example, the user could verify his identity by confirming something that the agency already knows about him but which is not common knowledge, such as tax return information. After verifying the user's identity, the registration authority creates a unique user name. This unique name, which may include the user's given name, ensures that people who rely on the certificate can distinguish between several individuals with similar given names, much like an e-mail address. The certification authority then creates the certificate that irrevocably links that unique name to the user's public key. Registration authorities focus on identifying and authenticating users; they do not sign or issue digital certificates. However, the registration authority is required to comply with preset standards for verifying a person's identity.

Because registration of large numbers of people in person can be expensive, in some situations an organization may determine that a less expensive registration process is adequate, even though the result would be a somewhat lower assurance of correct authentication. Regardless, a critical link in any PKI is the binding process used to associate the user with the user's public key. PKIs implemented by separate organizations, such as individual federal agencies, can be combined to create a larger interconnected system, such as a government wide, national, or international PKI. To do this, entities within each component system need a way to reliably establish an electronic path to the certification authorities that generate digital certificates for users within the other component systems. There are three major approaches, or certification path models, for doing this. First, the trust list method relies on all components accepting a specific list of trusted certification authorities. This approach is used by Web browsers. Second is the hierarchical model, in which a single "root" certification authority issues certificates to subordinate certification authorities located in each component system. Third is a mesh architecture, in which nonhierarchical links are established among certification authorities in separate components that are not subordinated to each other. For a complete discussion of these three different certification path models, see our report on the PKI issues.[9]

[9] GAO-01-277.

Implementation Policies Establish Trust Levels for PKIs

Organizations may choose varying levels of trust for different kinds of transactions or other electronic functions. As noted, one organization may require users to register for their digital certificates by visiting the registration authority in person, while another may allow users to register by providing identifying information online. One organization may require that users protect their digital certificates with a more secure hardware device, such as a smart card, while another may be satisfied with a less secure software storage device. One organization may require that the digital certificate itself contain certain information that limits the size and scope of the electronic transaction while another may not put any limits on the use of the certificate. Each agency will have to develop its own implementation policies to meet the requirements of its particular business model for electronic transactions using PKI and set forth in its implementation policies what types of certificates it will issue or accept. Two documents, called the certificate policy and the certification practices statement, are usually employed to provide these policies.

The certificate policy is a set of rules governing the intended use of certificates and the level of trust that a particular PKI will support. It contains items such as the obligations of the certification authority, its liabilities and warranties, confidentiality policy, identification and authentication requirements, and details of what information will be contained in the certificates. The certificate policy provides the criteria that can be used by others to determine whether to trust certificates issued by the certification authority and is also the basis for accreditation of the certification authority. The second document, called a certification practices statement, contains a more detailed description of the mechanics followed by a certification authority in issuing and otherwise managing certificates. It outlines the procedures used to implement the policies with regard to certificate issuance, user identification and registration, certificate lifetimes and revocation, and publishing practices for certificates and certificate revocation lists. It also states the operational practices followed by the certification authority to ensure security. The certification practices statement is used to outline operational procedures for the certification authority's personnel and also provides additional information to the relying party.

Attributes of Valid Electronic Signatures and Their Use in PKIs

Since the early 1980s, GAO has reviewed systems generating electronic signatures that are used in financial management systems. In performing this work, we reviewed the role that a signature plays in a traditional paper-based system when that signature is used as evidence of an intent to bind an individual to a given transaction. On the basis of what we found, we identified a set of technology neutral attributes of a valid signature acceptable for use in financial management systems.[10] Using these

[10] U.S. General Accounting Office, *Maintaining Effective Control over Employee Time and Attendance Reporting*, GAO-03-352G (Washington, D.C.: January 2003).

attributes, we stated that electronic signature systems are adequate to provide evidence of an agency's intent to be bound to financial transactions when the signatures generated by those systems are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if the data are changed, the signature is invalidated upon verification.[11] These criteria are technology neutral,[12] and the cryptographic properties associated with digital signature technologies can be used to develop and implement a public key-based system that has the ability to meet these criteria. These criteria also comply with the definition of an electronic signature in Section 1710 of GPEA, which states that the term "'electronic signature' means a method of signing an electronic message that—(A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message."

Risks Associated with Certification Authorities

As noted in your letter, several agencies have stated that GAO is concerned about whether a commercially managed service PKI could be used for their encryption needs. In our discussions, we have told the agencies that what they should be most concerned about are the increased levels of risks associated with this environment. We also told the agencies that until we could review the specific controls used by a given solution, we would be unable to express an opinion on the adequacy of a particular internal control solution. However, we expressed concerns about whether the internal control structure normally associated with commercially hosted services as described to us would be adequate when the certificates generated by those services were used as evidence of a federal agency's intent to be bound to a financial management transaction. The concerns that we raised are similar to those we would raise should a federal agency implement a certification authority using similar procedures. To date, no agency has requested that we undertake the review necessary to provide our opinion on whether a specific commercial solution would provide adequate controls to address our internal control concerns.

Certification authorities, when used to bind agencies, their employees, and others contracting with agencies for financial management transactions, are a critical component of a PKI regardless of whether a federal or commercial entity operates the certification authority because of the importance that the certification authority has in the PKI trust model. As discussed earlier, the certification authority is the entity that the other users of the PKI trust to guarantee the association between a public key and a specific user or entity. Accordingly, if the certification authority is compromised the impacts can be catastrophic to an agency's operations. This is especially true if the compromise is not immediately detected for some period of time since improper certificates could be issued to individuals or organizations that could

[11] See U.S. General Accounting Office, *Corps of Engineers Electronic Signature System*, GAO/AIMD-97-18R (Washington, D.C.: November 19, 1996) and U.S. General Accounting Office, *State Electronic Signature System*, GAO/AIMD-00-227R (Washington, D.C.: July 10, 2000).

[12] The last of the four criteria applies to electronic media.

be used to make improper payments for one or many improper transactions. Since all parties trust the certificates issued by the certification authority, an undetected compromise may, depending on what other controls are present, result in the systems that rely on those certificates making improper payments. For example, a financial management system may rely on a contracting officer's certificate to ensure that an obligation is valid before entering it into its records. The financial management system may also rely on a certificate issued to another individual to validate that the goods and services associated with that contract have been received and accepted by the agency. Once the financial management system is notified that an invoice has been received for these goods and services, it may automatically generate a payment since (1) a valid obligation has been recorded, (2) the goods and services called for in the obligating document have been received and accepted, and (3) an invoice has been received. This is a classic automated three-way match that leading financial management systems perform to reduce the costs associated with payment processing.[13] Simply stated, because of the trust the system places in the certificates issued by the certification authority, the system may securely transmit an improper payment based on the compromise. Once an agency has detected the compromise, it must take actions to attempt to collect any improper payments.

Even if the compromise is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of funds occurs from the compromise. As we have noted, systems must be set up to positively identify internal and external users, issue them digital certificates, and manage the exchange and verification of certificates. Should the certification authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the agency's policies and procedures. Certificates used for critical financial management applications should be issued based on split knowledge and dual control concepts and the individual's identity should be validated by personally appearing before the registration authority. For some agencies a compromise could mean reissuing tens of thousands certificates. If an agency has integrated its PKI into its systems, a significant disruption can result if the agency has to shut down associated systems because of a compromised PKI. For example, users may not be able to use those systems until they have received new certificates. In a non-PKI context, when one agency decided to shut down its financial management operations so that it could convert to a new system, we understand that the agency incurred over $1 million in late payment penalties as a result of the financial management system not being available. When the system has PKI, even if the agency bypasses the existing control process, the agency exposes itself to other attacks since the system is no longer using one of its critical control techniques to ensure data integrity—the PKI. Regardless of the decision, the agency is exposing itself to increased risks by (1) not processing transactions or (2) processing transactions without an adequate level of data integrity. As we have noted, procedures for exception processing need to be carefully planned since exception

[13] U.S. General Accounting Office, *Streamlining the Payment Process while Maintaining Effective Internal Control*, GAO/AIMD-21.3.2 (Washington, D.C.: May 2000), provides additional information on payment processing.

processing that is not as good as the primary process can be exploited as a security hole.[14]

In cases where a certification authority is compromised, the agency should have recovery plans in place to mitigate the damage. As a part of each agency's information security program which OMB must approve, agencies are required to have plans and procedures to ensure continuity of operations for information systems that support agency operations and assets, regardless of whether those operations and assets are managed by another agency, contractor, or other source.[15] Though necessary to ensure continuity of operations, the implementation of a plan to address the compromise and recover the necessary PKI functionality may likely cause an agency to incur significant costs.

Special Risks When Commercial Activities Host Certification Authorities

Pursuant to GPEA, the Justice Department (Justice) issued guidance that identifies issues that need to be addressed when using contractors to perform critical record-keeping functions. Justice stated that "agencies should ensure: (1) that an electronic process collects all relevant information; (2) that the information is retained properly; and (3) that the information is readily accessible" to ensure the availability of information in an electronic process. It also noted that the "potentially lengthy period of time between the collection of information and its use in many situations, including litigation, highlights the importance of these issues."[16] Maintaining and securing proper electronic records is an important function of the certification authority.

The Justice document recognized that "creative strategies can address some agency information management needs, such as ensuring the accessibility or the reliability of information." However, it noted that the use of outside parties to perform data storage functions traditionally performed by agency personnel can also create a variety of additional risks that should be carefully considered before turning over an agency's files to a private party. The Justice document outlined a number of actions that would need to be taken to provide the agency with reasonable assurance that the contractor adequately protects its electronic records. These steps included (1) choosing outside parties with care, (2) clearly outlining responsibilities before initiating the relationship, (3) placing reliance on an outside party only gradually, (4) closely monitoring the outside party, (5) regularly revisiting the nature and success of the relationship, (6) taking advantage of appropriate industry standards, and (7) developing backup plans.

[14] U.S. General Accounting Office, *Information Security: Challenges in Using Biometrics*, GAO-03-1137T (Washington, D.C.: September 9, 2003).
[15] 44 U.S.C. § 3544(b)(8).
[16] U.S. Department of Justice, *Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* (Washington, D.C.: November 2000).

When a third party operates a certification authority, the federal agency is highly dependent on the provider's system of internal controls over such items as software development, physical security decisions, and operations management. Justice noted that agencies should especially consider the regular use and reuse of auditing or certification procedures to examine whether the outside party is following appropriate practices and that other steps may be helpful as well in reducing particular risks associated with the use of outside parties. The report noted that in a recent case where at least 43,000 electronic messages were "lost," there was a misunderstanding between the agency, which believed that backups were being made both on a daily basis and a periodic systemwide basis, and the agency's contractor, which had been doing neither. A contributing factor to the loss of the messages may have been that the audit log features had been turned off to improve system performance. The practice of relying on a contractor to perform certification authority functions is very similar to relying on a commercial off the shelf (COTS) system. Because internal control structures for PKI should be developed in accordance with the specific needs of each agency, it is not clear whether commercial products, as we have generally discussed with agencies, can meet the internal control standards necessary to properly manage risk as outlined in the following section.[17]

Examples Of Internal Controls Associated with Issuing Certificates

The exact internal control structure needed for a given PKI should be developed based on an effective risk management approach that uses quantitative and qualitative factors. We have also found it useful to frame the discussion of a conceptual system approach around the control objectives that should be accomplished by the system. This process allows an evaluation that does not specify a given architecture and allows an agency to implement a solution that best meets its needs. The following examples of the types of control objectives that we might look for in reviewing a PKI for audit purposes are derived from various sources, including our internal control standards, OMB's Circular A-130, Appendix III, and GSA's Federal Bridge Certification Authority's practices statement:

- Split knowledge and dual control should be utilized to ensure that certificates issued to a given user are authorized and proper. Since a certificate is the means used to ensure that a given user electronically signed a given message, it is critical that the process used to link a certificate with a given user ensure that at least two different entities authorize the issuance of a given certificate in order to ensure that only the signer can generate a given signature. As noted in our *Standards for Internal Control in the Federal Government*,[18] key duties and responsibilities need to be divided or segregated among different people to reduce the risk of

[17] In a related matter, a Department of Defense study on COTS acquisitions found that the marketplace, not the program manager, drives development of the commercial item and that development of commercial items is driven primarily by the vendors' perceptions of what will sell to the largest number of potential users. Department of Defense, *Commercial Item Acquisition: Considerations and Lessons Learned*, (Washington, D.C.: June 26, 2000).

[18] U.S. General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, and reviewing the transactions, i.e., no one individual should control all key aspects of a transaction or event. Having one individual, such as a user's supervisor, notify the certification authority that a certificate should be issued to a given entity and having another individual, such as the registration authority, notify the certification authority that the agency prescribed policies and procedures for identifying that user have been followed help to accomplish this objective since a rogue registration authority does not have the ability to generate unauthorized certificates unless someone else authorizes the transaction. In addition, another individual should monitor the certificate issuance and maintenance processes to help ensure the integrity of the certification authority processes.

- The certification authority should log the critical certification authority activities, e.g., certificate generation requests, certificate revocation, rejected transactions, and requests to obtain keys used to decrypt data[19] in a manner that will detect deliberate or inadvertent modification of the data. The maintenance of adequate audit logs is critical to an effective PKI solution since these logs are used to help ensure that the prescribed policies and procedures and the resulting controls have been effectively implemented. For example, having the registration authority and another individual send electronically signed messages to the certification authority that a given certificate should be issued and then saving these signed messages in an audit log provides assurance to (1) the certification authority that at least two properly authorized individuals have approved the issuance of a certificate and (2) the system administrator and external reviewers that the certification authority is only issuing certificates to authorized individuals since the certification authority lacks the information to generate the necessary electronic signatures in a properly designed system.

- Cryptographic modules used for certification authorities should have adequate controls to ensure that the critical keying material is properly protected from unauthorized disclosure. By its very nature, a PKI depends on cryptographic modules to perform their critical functions. Because of the important role that the certification authority plays in the PKI trust model, it is critical that its cryptographic operations be performed without compromise and that the cryptographic keys be maintained under split knowledge and dual control when the cryptographic module does not protect them. Accordingly, we believe that, for certain applications,[20] the cryptographic module used in certification authorities should be hardware based and validated to comply with at least the level 3 criteria specified in the Federal Information Processing Standard (FIPS) 140-2—*Security*

[19] In order to ensure that the user has sole control over the key used to generate electronic signatures used to bind an individual, the key should only be stored in a cryptographic device under that user's sole control. In other words, keys for signing documents should not be archived or stored in a device that is not under that user's sole control. On the other hand, the keys needed to decrypt a message should be archived and provided to authorized parties should the need arise. For example, a user may lose the token containing the encryption key and be unable to read messages encrypted with that encryption key until that key is restored to a new token.

[20] Certification authorities used to generate federal agency certificates that are used in financial management applications is one example.

Requirements for Cryptographic Modules[21] since the level 3 requirements contained in FIPS 140-2, coupled with the process to validate that these modules comply with the given standards, allows an agency to obtain reasonable assurance that critical controls such as key generation, key storage, and algorithm compliance with standards are met by this critical piece of the PKI.

- Physical control of the certification authority's critical hardware and software should remain under federal agency control. The number of attacks that can be launched against a certification authority can be reduced if the attacker does not have physical access to the device. For example, if agency personnel obtain and install the hardware and software used, they can implement a process to ensure that these items come from trusted sources and that the devices have not been modified in such a manner that would compromise their operations. This should not be construed to mean that an agency cannot physically locate its certification authority on the premises of a contractor. As noted earlier, the Justice Department has outlined a number of factors that must be addressed when contracting out critical functions relating to agency record keeping. We believe that the items identified by Justice apply to certification authorities. Accordingly, should an agency decide that it would like to contract out its certification authority functions, it should comply with the Justice guidelines and ensure that the controls provide the same degree of assurance that would be present if the agency maintained physical access and control over the certification authority.

These control objectives have been outlined in executive branch documents. For example, in a document developed for the Department of Energy for its PKI,[22] NIST outlined similar control objectives and security requirements that a certification authority should perform. The control objectives outlined above are also similar to those contained in the Federal Bridge Certification Authority's practices statement.[23] It requires that all software and hardware installed in or run on its certification authority be purchased using an accountable method of packaging and delivery that will be used to provide a continuous chain of accountability from the vendor to the facility and that installation is performed under multi-person control with only Federal Bridge Certification Authority authorized personnel.

In addition to using these control objectives, agencies can use documents produced by NIST to help assess their risks and identify appropriate control techniques to address those risks. Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST to develop:

- standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based

[21] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, MD: May 25, 2001).

[22] National Institute of Standards and Technology, *PKI Specifications to Support the DoE Travel Manager Program*, (Gaithersburg, MD: August 15, 1996).

[23] General Services Administration, *Public X.509 Certification Practice Statement (CPS) for the Federal Bridge Certification Authority (FBCA)*, (March 7, 2003).

on the objectives of providing appropriate levels of information security according to a range of risk levels;

- guidelines recommending the types of information and information systems to be included in each such category; and
- minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.

The documents that NIST has developed in response to these tasks can be found at http://csrc.nist.gov/sec-cert/ca-library.html.

Commercial Certification Authority Control Environment Discussed with Agencies

Our limited understanding of the commercially managed solutions is consistent with the information contained in your letter, which states that these services allow the agency to outsource the technical operations of the certification authority while allowing the government to maintain full control over certificate registration and policies. We recognize that one reason that an agency may want to contract out the operation of a certification authority is because the agency does not believe that operating a certification authority is one of its core competencies.[24] Contracting out the mechanics of certificate issuance is only a part of the cost of a PKI. The labor-intensive process costs associated with user registration will still be borne by the agency. In addition, the agency will have to integrate the PKI security features into its applications. As we noted in our February 2001 report, developing, implementing, and enforcing a complete set of policies and procedures is likely to require a substantial effort on the part of each agency. Even if agencies contracted out the mechanics of certificate issuance, as noted in your letter, they would still be responsible for the costly user registration and security processes.

Using a certification authority where the registration process is handled by the agency while a contractor handles the certificate issuance requires the agency to understand the risks that are being undertaken and whether the strong binding that may be required by the agency during registration is maintained throughout the certificate issuance process. As we noted earlier, to date, we have not formally been requested by an agency to review a commercial service provider's system. However, on the basis of our informal discussions, we have some concerns on whether the models that have been discussed with us maintain a strong binding.

[24] Core competencies can be defined as those specific areas of knowledge and expertise that the agency considers vital to its success. In may be argued that the agency can obtain better results from areas that are not part of its core competencies by using service providers that deliver such services through their own core competencies. However, agencies still need to have sufficient expertise to oversee the contractors that it hires to perform these services.

One conceptual approach for a commercial certification authority that has been discussed uses the following process to issue a certificate:

- User appears before the agency's registration authority that follows the prescribed policies to ensure that the user should be issued a certificate.

- Registration authority logs onto the commercial certification authority via the Internet over an encrypted channel using a user identification code and password.

- After authenticating the registration authority by using the registration authority's user identification code and password, the commercial certification authority issues the requested certificates to the user, e.g., a digital signature certificate and a certificate that can be used for data encryption.

This model has several risks that can weaken the link between the registration process and the resulting certificate. These include:[25]

- The certificate is issued based solely on the representation by a registration authority that the certificate should be issued to a given user. This would allow a rogue registration authority to generate unauthorized certificates. It is our understanding that the commercial certification authority is not responsible for any liabilities associated with certificates that were issued improperly based on information obtained from a registration authority.

- The authentication of the registration authority to the certification authority is based on user identification codes and passwords. This is a weak form of authentication and allows the certification authority (or someone who has gained unauthorized access to this system) to have the knowledge necessary to masquerade as the registration authority since it can easily obtain a given user's authentication information. Therefore, it may be very difficult to determine whether a given registration authority actually requested a given certificate or to prove that the registration authority did request a given certificate. The complexity of the problem is increased since the commercial provider will maintain and be able to control all the records necessary to "prove" who performed a given action.

Although we have not been asked by a federal agency to review a given commercial solution, as discussed in the previous section, we have given some thought to the functionality that should be provided by a certification authority and the conceptual types of controls needed to ensure that the certificates generated are adequate to bind a user to that user's certificates.

[25] Although these are examples, not all of the risks associated with a certification authority may be known at this time. Therefore, agencies conducting a risk analysis of certification authorities need to adopt a process that will be able to ensure that the significant risks for a given application have been properly identified.

Commercial Certification Authorities Play a Role in a Federal Agency's PKI

Several federal agencies use products that perform certification authority functions that have been developed by the private sector. It is our understanding that these agencies have acquired the commercial product and then installed it in a federal facility with federal personnel holding security clearances performing the critical functions. These activities may also use contractors to help maintain the system. Assuming that adequate controls have been implemented over this process, this approach should be able to adequately address the risks associated with a certification authority.

Agency use of certificates generated by commercial activities also has the potential to adequately address the risks associated with a certification authority that is not under the total control of a federal agency. For example, a common method of facilitating secure transactions through the Internet is to use a protocol known as the secure sockets layer (SSL) to encrypt the data that are transmitted between a user's computer and an electronic commerce Web site. A PKI certificate is used in this process in order for the browser to authenticate the server that the browser is connecting with and establishing an encrypted session between the user's browser and the server. Federal agencies, such as the United States Mint, use certificates issued by commercial entities to establish these connections for their e-commerce activities. In addition, a federal agency may need to conduct business with a private sector counterpart that only has a certificate issued by a private sector entity. The federal agency, after conducting an appropriate risk analysis, may conclude that the certificates used by the private sector entity provide reasonable assurance that those certificates are adequate to bind the private sector entity to a given type of transaction. For example, an agency may desire that a vendor submit a bid proposal and digitally sign the proposal in such a manner that would commit the vendor to the information contained in that proposal. Rather than issuing all potential vendors certificates so that this can be accomplished, the agency may decide that a given type of certificate issued by commercial certification authorities is adequate based on the agency's risk analysis. The exact process that should be used by agencies making this determination is beyond the scope of this letter.

As agreed with your office, unless you announce the contents of this report earlier, we will not distribute it until 30 days after its date. At that time, we will send copies to other interested congressional committees. We will also be sending copies to the Director, Office of Management and Budget. Copies of this report will be made available to others upon request. The report is also available at no charge on GAO's Web site at http://www.gao.gov.

- - - - -

If you have any questions concerning this report, please contact me (202) 512-6412 or by e-mail at rhodesk@gao.gov or Chris Martin, Senior Level Technologist for Cryptography and Systems Development, at (202) 512-9481 or by e-mail at martinj@gao.gov.

Sincerely yours,

Keith A. Rhodes
Chief Technologist
Center for Technology and Engineering

(460573)

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER