USDA

U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Review of Public Key Infrastructure at the Office of the Chief Financial Officer/National Finance Center

Report No. 11099-45-FM
October 2004

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: October 29, 2004

REPLY TO
ATTN OF: 11099-45-FM

SUBJECT: Review of Public Key Infrastructure at Office of the Chief Financial Officer/National Finance Center

TO: Patricia E. Healy
Acting Chief Financial Officer
Office of the Chief Financial Officer

ATTN: Kathy Donaldson
Audit Liaison Officer
Office of the Chief Financial Officer

This report presents the results of our audit of the U.S. Department of Agriculture's Review of Public Key Infrastructure at Office of the Chief Financial Officer/National Finance Center. The Office of the Chief Financial Officer's response to the official draft, received on October 18, 2004, is included in its entirety as exhibit C with excerpts and the Office of Inspector General's position incorporated into the Findings and Recommendations section of the report.

Based on the information contained in the response, we have reached management decision on all recommendations and, therefore, no further correspondence with our office is necessary. If you have any questions, please contact me at 202-720-6945, or have a member of your staff contact Richard Davis, Director, Administration and Finance Division, at 202-720-1918.

We appreciate the cooperation and courtesies extended to us during this review.

/s/

ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Review of Public Key Infrastructure at Office of the Chief Financial Officer/National Finance Center

Results in Brief

We reviewed the public key infrastructure (PKI) maintained by the U.S. Department of Agriculture, Office of the Chief Financial Officer (OCFO), National Finance Center (NFC), with specific emphasis on the certification authority function. A certification authority is responsible for managing digital certificates, which can be used to confirm the identities of parties sending and receiving electronic payments or other communications. Our objectives were to determine whether the NFC certification authority operated in compliance with its documented practices, those practices were in compliance with Federal requirements, and controls over certain PKI operations were adequate.

We found that the NFC certification authority was in substantial compliance with its documented practices and Federal requirements for operating as a PKI shared service provider. The practices documented in NFC's April 2004 PKI certification practices statement adequately addressed all but two of the about 150 applicable Federal requirements and the NFC certification authority had implemented all but three of the provisions in its documented practices. (These three provisions had been added to the statement to meet February 2004, issued Federal requirements.) Subsequent to our fieldwork, NFC implemented four of these five outstanding requirements. NFC officials told us that the remaining requirement would be completed by December 31, 2004. NFC has been fully certified as a PKI shared service provider for the Federal Government.

We also identified two areas where NFC could improve general controls that were not specifically mentioned in its documented practices. NFC's certification authority had not fully apprised its subscribers, or officials performing the local registration authority function, of their roles and responsibilities or adequately documented the tests it ran on its plan for continuing PKI operations in the event of an unexpected system disruption. Subsequent to our fieldwork, NFC updated subscriber and local registration authority agreements and user guides to address our concerns.

Recommendations In Brief

We recommended that NFC complete planned actions to implement the final Federal requirement for operating as a PKI shared service provider. We also recommended that NFC establish procedures for planning, documenting, and reviewing the results of its PKI continuity of operations testing.

Agency Response OCFO/NFC agreed with the findings and recommendations in this report.

OIG Position We concur with the management decisions.

Abbreviations Used in This Report

e-Gov	Electronic Government
FBCA	Federal Bridge Certification Authority
FICC	Federal Identity Credentialing Committee
LRA	Local Registration Authority
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
UMARS	USDA Management and Registration System
USDA	United States Department of Agriculture

Table of Contents

Background and Objectives

Background

Increasingly, Federal agencies are moving to Electronic Government (e-Gov) to facilitate their interaction with citizens and businesses and improve efficiency and effectiveness. E-Gov can include activities such as information collection and dissemination, funds and benefits transfers, filings and applications, revenue collection, and procurement of goods and services. E-Gov offers the potential for improvements in service delivery and productivity. However, it also introduces increased threats and risks. Unless special security features are properly implemented, electronic transactions are much more susceptible to fraud and abuse than paper-based transactions.

National Institute of Standards and Technology (NIST) guidance[1] states that, where there is a need for a secure transaction, individuals or entities interacting electronically with Federal agencies should have four kinds of security assurances: identification and authentication, confidentiality, data integrity, and nonrepudiation.[2] If fully and properly implemented, public key infrastructure (PKI) can provide these types of assurances so that sensitive Government transactions can be adequately secured.

The basis of PKI's security assurances is a sophisticated cryptographic technique known as public key cryptography, which uses two keys—a public key and a private key. This key pair is mathematically related so that given the public key, it is computationally infeasible to derive the private key. Public key cryptography can be used for encryption, which provides confidentiality, or digital signatures, which provide authentication, data integrity, and nonrepudiation. For security reasons, separate key pairs are generated for encryption and digital signatures.

- An encryption key pair consists of an encryption public key and a decryption private key. The public key portion of an encryption key pair is used to encrypt data that can be decrypted by the matching decryption private key.

- A signing key pair consists of a signing private key and a verification public key. The public key portion of a signing key pair is used to verify data that has been signed by the matching signing private key.

In both cases, the private key must remain secret and the public key is made publicly available, normally in the form of a digital certificate.

[1] NIST Special Publication 800-25, "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication," September 2000.
[2] Nonrepudiation provides proof of the integrity and origin of data that can be verified by a third party and may provide important legal evidence in the event of a dispute.

A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity. It is created by placing the entity's name, public key, and other identifying information in a small electronic document that is stored in a database. A trusted third party called a certification authority digitally signs the certificate to provide assurance that the public key contained in the certificate belongs to the entity named in the certificate.

The certification authority is responsible for managing digital certificates, which can be used to confirm the identities of parties sending and receiving electronic payments or other communications. The certification authority oversees the generation, distribution, renewal, revocation, and suspension of digital certificates. It is also responsible for providing certificate status information because digital certificates may expire or be revoked. Before the certification authority can issue a certificate to a user, it must verify the user's identity. In some cases, the certification authority is set up to perform the identification and authentication of users, but often this function is delegated to separate entities called registration authorities. Users of PKI are usually classified as certificate holders (e.g., subscribers) or relying parties that use PKI components to verify certificates of other entities and to know, with certainty, the public key of another subscriber.

PKI requirements and practices for certification authorities are generally defined in two documents: a certificate policy and a certification practices statement. The certificate policy sets forth the general requirements for PKI subscribers and relying parties and describes the appropriate uses for certificates. The certification practices statement is typically a comprehensive statement of practices and procedures that a certification authority employs in issuing, suspending, revoking, and renewing digital certificates and providing access to them. Where a certificate policy sets forth general requirements, a certification practices statement explains how a certification authority meets the requirements of the policy.

Recognizing that many Federal agencies had set up independent certification authorities, the Federal Bridge Certificate Authority (FBCA) was established to allow disparate agency PKIs to interoperate and to link unconnected certification authorities into an overall Federal PKI. FBCA cross-certifies authorities based on policies that establish requirements for four assurance levels: rudimentary, basic, medium, and high.

It is the intention of the Federal Government to centralize processes for deployment of PKI. The Federal Identity Credentialing Committee (FICC) is in the process of selecting managed service providers (also referred to as shared service providers) that will operate under a common Federal PKI certificate policy[3] that implements a level of assurance comparable to or

[3] The common Federal PKI certificate policy is more formally known as the X.509 Certificate Policy for the Common Policy Framework, which was issued in February 2004.

greater than the FBCA medium assurance policy. FICC has designated the National Finance Center (NFC) as a certified shared service provider for the Federal Government.

The NFC certification authority serves Federal agencies and their business related entities by offering certificates that meet the FBCA basic and medium levels of assurance. After entering into a service level agreement with the NFC certification authority, participating agencies designate a local registration authority (LRA) to perform the necessary verification procedures for the participating agency employees who will receive certificates from the NFC certification authority.

Objectives

Our initial audit objective was to determine if NFC controls over key and certificate life cycle management were adequately designed and operating effectively. However, at our entrance conference, NFC officials requested that we expand our audit procedures to determine if NFC practices were (1) consistent with the requirements set forth in its certificate policy and (2) in compliance with the requirements in its certification practices statement and signed service level agreements. During our fieldwork, NFC officials also requested that we determine if its certification practices statement was in compliance with the common Federal PKI certificate policy.

Finding 1 Federal and NFC PKI Requirements Were Substantially Met

NFC was in substantial compliance with Federal requirements for operating as a PKI shared service provider and with its documented practices. NFC's April 2004 certification practices statement adequately addressed all but 2 of the about 150 applicable Federal requirements and NFC had implemented all but 3 of its documented practices. Subsequent to our fieldwork, NFC implemented four of these five outstanding requirements. However, until the final issue is addressed, NFC will not fully comply with the requirements for operating as a PKI shared service provider for the Federal Government.

In March 2004, requirements[4] for becoming a PKI shared service provider for the Federal Government were issued. These requirements state that an independent auditor must determine if (1) the shared service provider's certification practices statement is in compliance with the common Federal PKI certificate policy and (2) the shared service provider's PKI is operated in compliance with its documented practices.

Compliance with Federal PKI Requirements

We compared NFC practices, as described in its April 2004 certification practices statement, with the requirements of the common Federal PKI certificate policy. We found that NFC practices satisfied all but 2 of the about 150 applicable Federal requirements. The two missing requirements are described in more detail in exhibit A. Subsequent to our fieldwork, NFC implemented one of the two outstanding requirements. NFC officials told us that the remaining provision required the NFC Certificate of Authority to discontinue support for a certain type of certificate that would impact customer operations and could not be adequately planned and implemented until December 31, 2004.

Compliance with NFC's Documented Practices

To determine if NFC was operating in compliance with its certification practices statement and signed service level agreements, we interviewed NFC personnel, observed certification authority practices, verified that certification authority components had been validated as meeting Federal standards, performed vulnerability scans of 32 PKI systems, and reviewed documentation provided by NFC. This included its certificate policy, certification practices statement, signed service level agreements, and

[4] These requirements have been defined by the Shared Services Provider Working Group, which is a subcommittee of FICC. Statutory authority is derived from the E-Government Act, passing from the Office of Management and Budget (OMB) through the Federal CIO Council (http://www.cio.gov/) to the FICC, and in turn to the FICC Shared Service Provider Subcommittee.

documentation associated with judgmentally selected samples of certificates that were issued, updated, or revoked between September 2002, when NFC received its authorization to operate, and January 2004.

Our initial audit work was based on the certification practices statement dated December 2003. We identified certain areas where NFC had not fully complied with the requirements of this statement. Examples of these areas are described in more detail in exhibit B. To address the problems we identified, NFC updated its certificate policy, certification practices statement, and procedures. Consequently, we concluded that, as of April 2004, (1) NFC's certification practices statement was consistent with its certificate policy and (2) the NFC certification authority was operating in compliance with the requirements of its certification practices statement and signed service level agreements.

In April 2004, NFC also updated its certification practices statement to address new requirements for becoming a shared service provider for the Federal Government. We evaluated these new requirements to identify areas that were not covered under our original testing. While NFC had satisfied some of the new provisions, it had not fully implemented three of the added requirements, which are described in more detail in exhibit A. Subsequent to our fieldwork, NFC implemented these three outstanding requirements.

Recommendation No. 1

Complete planned actions to implement the final Federal requirement for operating as a PKI shared service provider. This requirement and planned actions are described in more detail in exhibit A.

Agency Response OCFO/NFC agreed with this recommendation. All requirements and planned actions described in exhibit A are either completed or will be completed by December 31, 2004.

OIG Position We concur with the management decision.

We also identified two areas where NFC could improve general controls over its PKI operations that were not specifically mentioned in its certification practices statement. Specifically, NFC had not fully communicated roles and responsibilities to its subscribers or officials performing the LRA function.[5] Subsequent to our fieldwork, NFC had taken action to address these issues.

Finding 2

LRA and Subscriber Roles and Responsibilities Were Not Adequately Communicated

NFC had not fully communicated the roles and responsibilities that LRAs and subscribers had as part of NFC PKI operations. NFC had created agreements to inform LRAs and subscribers of their roles and responsibilities and user guides to provide training on the U.S. Department of Agriculture Management and Registration System (UMARS). However, these agreements and user guides were incomplete. NFC officials told us that these documents were initially issued to provide guidance for the creation of new certificates and had not yet been updated to include additional functions that could be performed through UMARS. Subsequent to our fieldwork, NFC updated the LRA and subscriber agreements and user guides to address these issues. According to NFC officials, the updated agreements and guides were provided to users in June 2004.

OMB Circular A-130 requires agencies to (1) establish rules that clearly delineate responsibilities and expected behaviors of all individuals with access to a system and (2) provide training focused on these responsibilities. In this regard, NFC requires LRAs and subscribers to sign an agreement in front of a witness to document acceptance of their responsibilities, which are documented in the certificate policy and in the certification practices statement. In addition, NFC relies on the UMARS user guide and LRA user guide to provide training for agency subscribers and LRAs.

We reviewed the agreements and user guides for LRAs and subscribers. While these documents appear to adequately address the creation of new certificates, they did not fully communicate the responsibilities specified in the certification practices statement or provide guidance on functions that LRAs and subscribers are expected to perform through UMARS after initial certificate issuance.

[5] LRAs perform certain registration authority functions for a local community. For the NFC certification authority, these functions include registering new subscribers, verifying the identity of subscribers and the accuracy of information included in certificates, requesting the issuance and/or revocation of certificates, and communicating activation codes for subscriber certificates.

- The LRA agreement and user guide did not inform LRAs of the requirement or provide guidance for performing a quarterly review of active subscribers, maintaining certain information (address, phone number, etc.) on the UMARS subscriber record, deleting UMARS subscriber records, reissuing activation codes for key recovery, or managing the number of licenses assigned to an individual user.

- The subscriber agreement did not communicate the timeframe requirements specified in the certification practices statement for initializing PKI credentials, notifying NFC of a suspected key compromise, or reporting changes to data included in certificates and/or certificate request forms.

- The UMARS user guide did not provide instructions for performing self-recovery of PKI credentials.

We also noted that the LRA and subscriber agreements incorporate the requirements specified in the certificate policy but direct these users to an incorrect web site to obtain this document.

Subsequent to our fieldwork, NFC updated the agreements to fully disclose the responsibilities specified in the certification practices statement and reference the correct web site for its certificate policy. NFC also updated LRA and user guides to include instructions that describe when and how to perform all functions available through UMARS. According to NFC officials, the updated agreements and guides were provided to users in June 2004. Consequently, we are not making any further recommendations.

Finding 3 Continuity of Operations Testing Was Not Consistently Documented

NFC had developed plans and procedures to provide continuity of operations and performed periodic tests to ensure that its PKI operations would not be significantly impacted by a system disruption. However, the agency had not consistently (1) developed formal test plans with objectives, procedures, and expected results or (2) documented the actual results of its PKI continuity of operations testing. NFC officials told us that, after the initial test, continuity of operations test objectives and results were discussed, but not formally documented because the process was substantially the same. Even so, formally documenting PKI continuity of operations test plans with objectives, procedures, and expected results would help NFC ensure that its PKI Continuity of Operations Plan is fully tested and updated when necessary.

The Federal Information Security Management Act requires agencies to develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. In addition, OMB Circular A-130 states that such plans should be tested. In October 2003, NIST issued draft recommended security controls for Federal information systems[6] that include provisions for documenting test results and providing them to appropriate officials for review.

We reviewed documentation maintained by NFC from the June 2002 PKI continuity of operations test. For this test, NFC documented the test scenarios that were performed and maintained audit logs to document that the tests were successful. Since the June 2002 test, NFC had transferred processing to its backup site in January 2003, May 2003, and March 2004, but had not documented test plans or results. NFC officials told us that the first test in June 2002 resulted in formal documentation, but subsequent tests were not formally documented because the processes for ensuring continuity of PKI operations were substantially the same.

NFC documented the results of their August 2004 PKI continuity of operations test, which occurred subsequent to our fieldwork. In addition, NFC told us that they would establish procedures, develop test plans, and document and evaluate the results of its PKI continuity of operations tests.

Recommendation No. 2

Establish procedures to (1) develop test plans with test objectives, test procedures, and expected results for tests of the PKI Continuity of Operations Plan; (2) document the actual results of PKI continuity of operations testing; and (3) evaluate these results to determine if the PKI Continuity of Operations Plan needs to be updated.

Agency Response

OCFO/NFC agreed with this recommendation. Testing plans, procedures, and expected results are currently being documented, as well as the evaluation of the results of tests previously conducted. Estimated completion date is November 30, 2004.

OIG Position

We concur with the management decision.

[6] Draft NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," October 2003.

Scope and Methodology

We performed our work at NFC, which is located in New Orleans, Louisiana, from December 2003 through April 2004, in accordance with Government Auditing Standards.

To accomplish our audit objectives, we (1) compared NFC's certificate policy with its certification practices statement, (2) compared NFC's certification practices statement with the common Federal PKI certificate policy, (3) held discussions with NFC officials, (4) observed NFC practices, (5) reviewed system documentation provided by NFC, and (6) performed tests to determine if NFC practices satisfied the requirements of its certification practices statement and signed service level agreements. Our testing included the following procedures:

- We verified that NFC certification authority components had been validated as meeting Federal Information Processing Standards.

- We reviewed samples of certificates that were issued, updated, or revoked between September 2002, when NFC received its authorization to operate, and January 2004. These samples were judgmentally selected to ensure that different types of certificates were included.

- We performed Internet Security Software scans to identify security vulnerabilities on the 32 servers at NFC that support PKI operations.

- We analyzed NFC firewall rules that restricted network traffic to and from its PKI systems.

- We evaluated the NFC PKI Continuity of Operations Plan and documentation maintained from tests of this plan.

Exhibit A – Compliance with Federal PKI Requirements

NFC's April 2004 certification practices statement adequately addressed all but two requirements in the common Federal PKI certificate policy. Specifically, the NFC certification authority key pair was 1024 bits rather than 2048 bits, as required by the Federal policy. NFC updated its certification authority key pair to 2048 bits in August 2004. In addition, the NFC certification authority sets the *dataEncipherment* bit for key usage[7] in a certain type of certificate due to customer requirements. However, the common Federal PKI certificate policy prohibits this key usage bit. NFC plans to discontinue support for this type of certificate by December 31, 2004.

In addition, NFC updated its April 2004 certification practices statement to address new requirements imposed by the common Federal PKI certificate policy. While NFC had satisfied some of the new requirements, it had not fully implemented the object identifiers[8] or LRA requirements added to comply with the common Federal policy. We also noted that the NFC certification authority had not yet changed the lifetime of its certificate from 10 years, which was required for operation under the policy for FBCA medium assurance, to 6 years as required by the common Federal PKI certificate policy. Subsequent to our fieldwork, NFC fully implemented these three provisions.

[7] Key usage bits specify how a public key in a certificate may be used. The *dataEncipherment* bit allows the public key in a certificate to be used for enciphering user data, but not keys or other security information.

[8] Object identifiers are specialized formatted numbers registered with an internationally recognized standards organization. In the Federal Government PKI, object identifiers are used to uniquely identify supported policies and cryptographic algorithms.

Exhibit B – Compliance with NFC PKI Practices

We identified certain areas where NFC had not fully complied with the requirements in its December 2003 certification practices statement. For example:

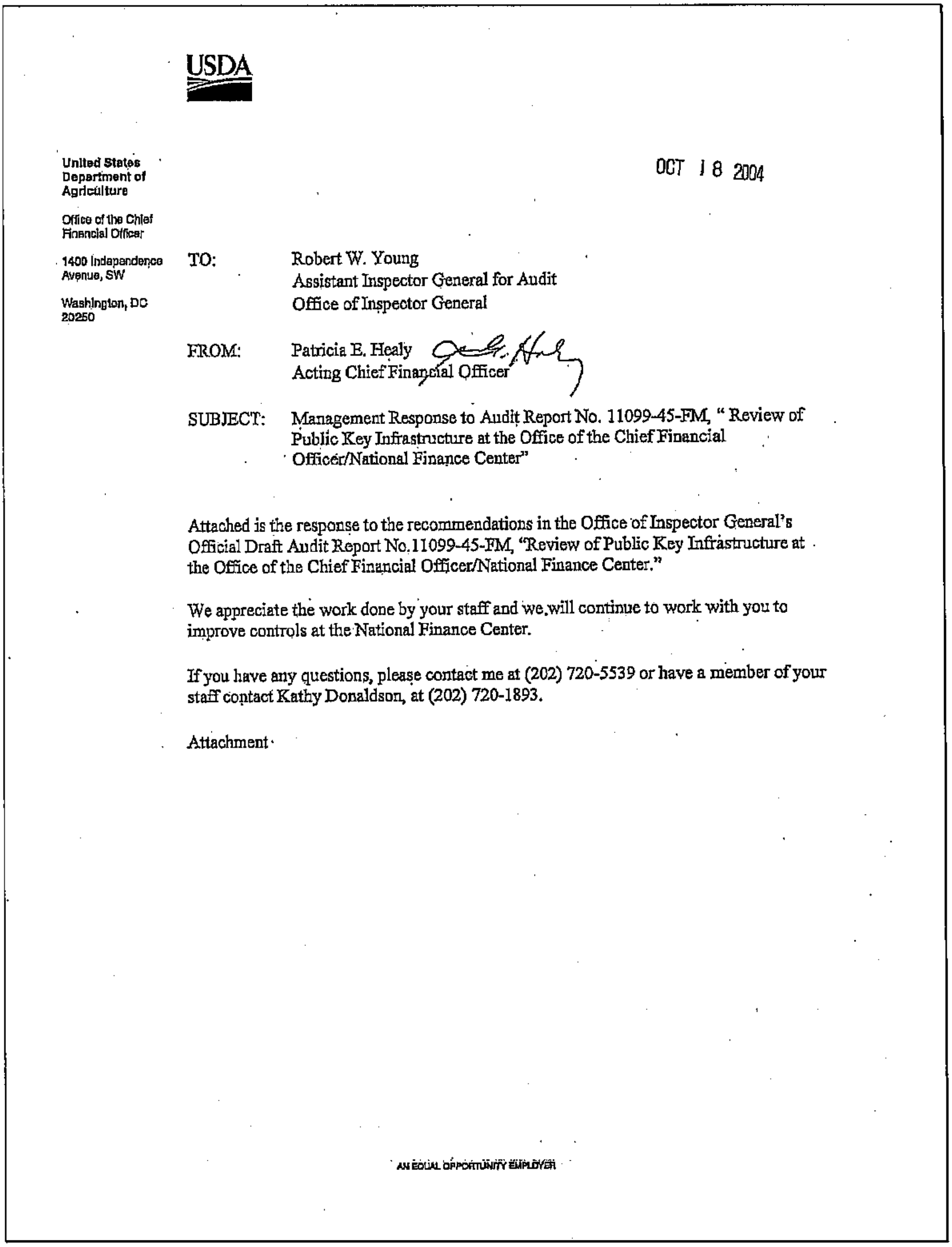
- NFC had not implemented the requirement that passwords have the shortest lifetime practical. NFC had set passwords so they would not expire and allowed users to use the same password over and over. This increased the risk that a password could be discovered and used to obtain improper access. Upon our notification, NFC set password expiration to 14 weeks and password history to 6 generations, which meets NIST requirements.

- NFC had not set the system option to take action after a predetermined number of failed login attempts. Allowing unlimited attempts to guess passwords increases the risk of unauthorized access. Upon our notification, NFC updated its system settings to suspend accounts after three failed login attempts, which meets NIST requirements.

- NFC had one high, two medium, and eight low vulnerabilities on one PKI server because a patch had been incorrectly applied. Even though NFC subsequently performed the same type of vulnerability scans that we performed, the NFC scans did not reveal the vulnerabilities because they were not conducted from within the PKI room. Upon our notification, NFC corrected the vulnerabilities. In addition, officials agreed to begin scanning the PKI servers on the secure segment of the network from within the PKI room to help ensure that all vulnerabilities are identified during the scans.

- NFC had issued 6 of the 20 certificates we reviewed before it had obtained all of the required documentation. NFC subsequently obtained the missing documentation for these certificates. However, to ensure that these types of problems would not recur, NFC officials told us that they had reminded their registration authority not to perform any actions until the proper documentation has been received. They also said they would begin annual training regarding PKI roles and responsibilities.

Exhibit C – Agency Response



USDA

United States
Department of
Agriculture

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

OCT 18 2004

TO: Robert W. Young
Assistant Inspector General for Audit
Office of Inspector General

FROM: Patricia E. Healy
Acting Chief Financial Officer

SUBJECT: Management Response to Audit Report No. 11099-45-FM, " Review of Public Key Infrastructure at the Office of the Chief Financial Officer/National Finance Center"

Attached is the response to the recommendations in the Office of Inspector General's Official Draft Audit Report No.11099-45-FM, "Review of Public Key Infrastructure at the Office of the Chief Financial Officer/National Finance Center."

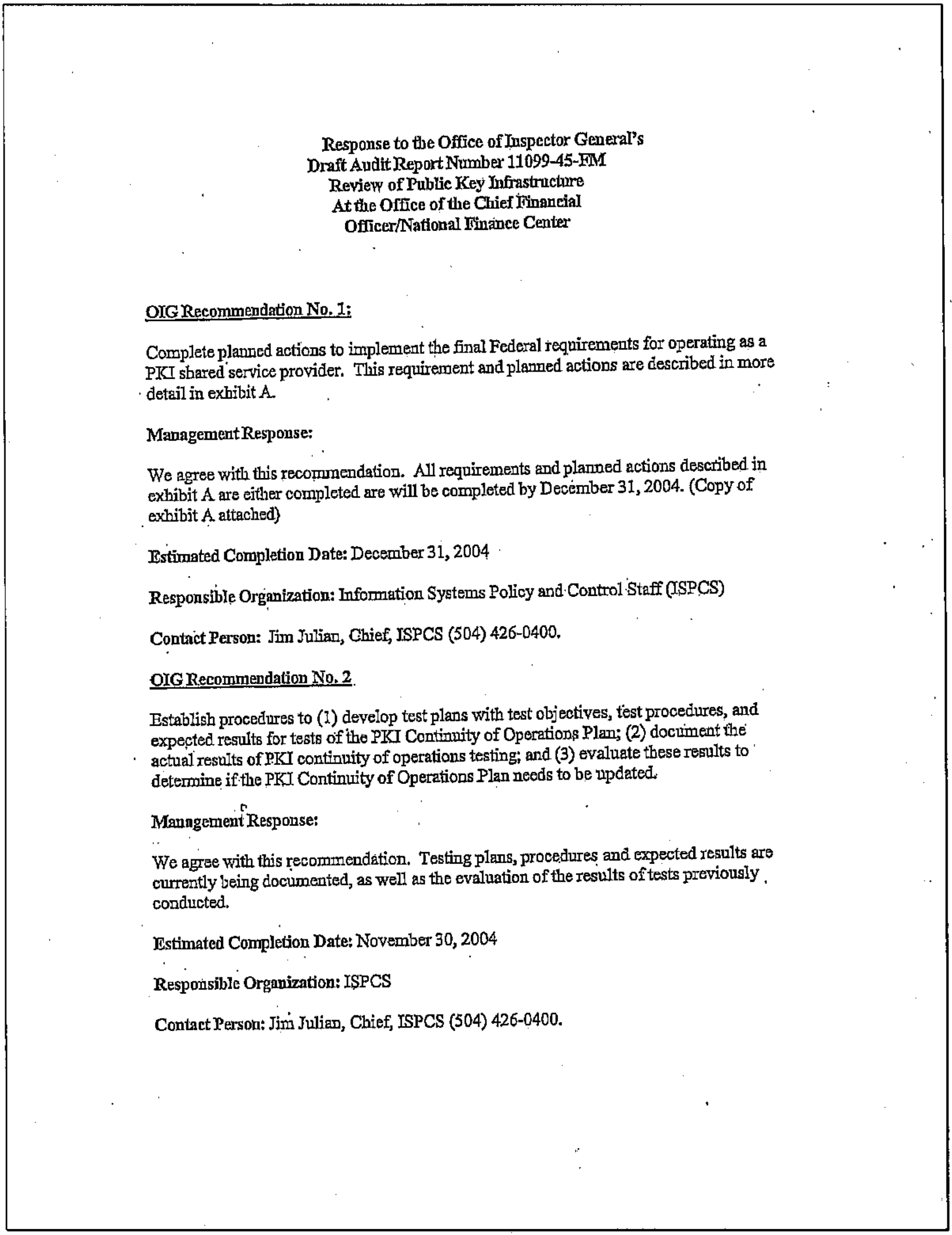
We appreciate the work done by your staff and we will continue to work with you to improve controls at the National Finance Center.

If you have any questions, please contact me at (202) 720-5539 or have a member of your staff contact Kathy Donaldson, at (202) 720-1893.

Attachment

AN EQUAL OPPORTUNITY EMPLOYER

Exhibit C – Agency Response



Response to the Office of Inspector General's
Draft Audit Report Number 11099-45-FM
Review of Public Key Infrastructure
At the Office of the Chief Financial
Officer/National Finance Center

OIG Recommendation No. 1:

Complete planned actions to implement the final Federal requirements for operating as a PKI shared service provider. This requirement and planned actions are described in more detail in exhibit A.

Management Response:

We agree with this recommendation. All requirements and planned actions described in exhibit A are either completed are will be completed by December 31, 2004. (Copy of exhibit A attached)

Estimated Completion Date: December 31, 2004

Responsible Organization: Information Systems Policy and Control Staff (ISPCS)

Contact Person: Jim Julian, Chief, ISPCS (504) 426-0400.

OIG Recommendation No. 2

Establish procedures to (1) develop test plans with test objectives, test procedures, and expected results for tests of the PKI Continuity of Operations Plan; (2) document the actual results of PKI continuity of operations testing; and (3) evaluate these results to determine if the PKI Continuity of Operations Plan needs to be updated.

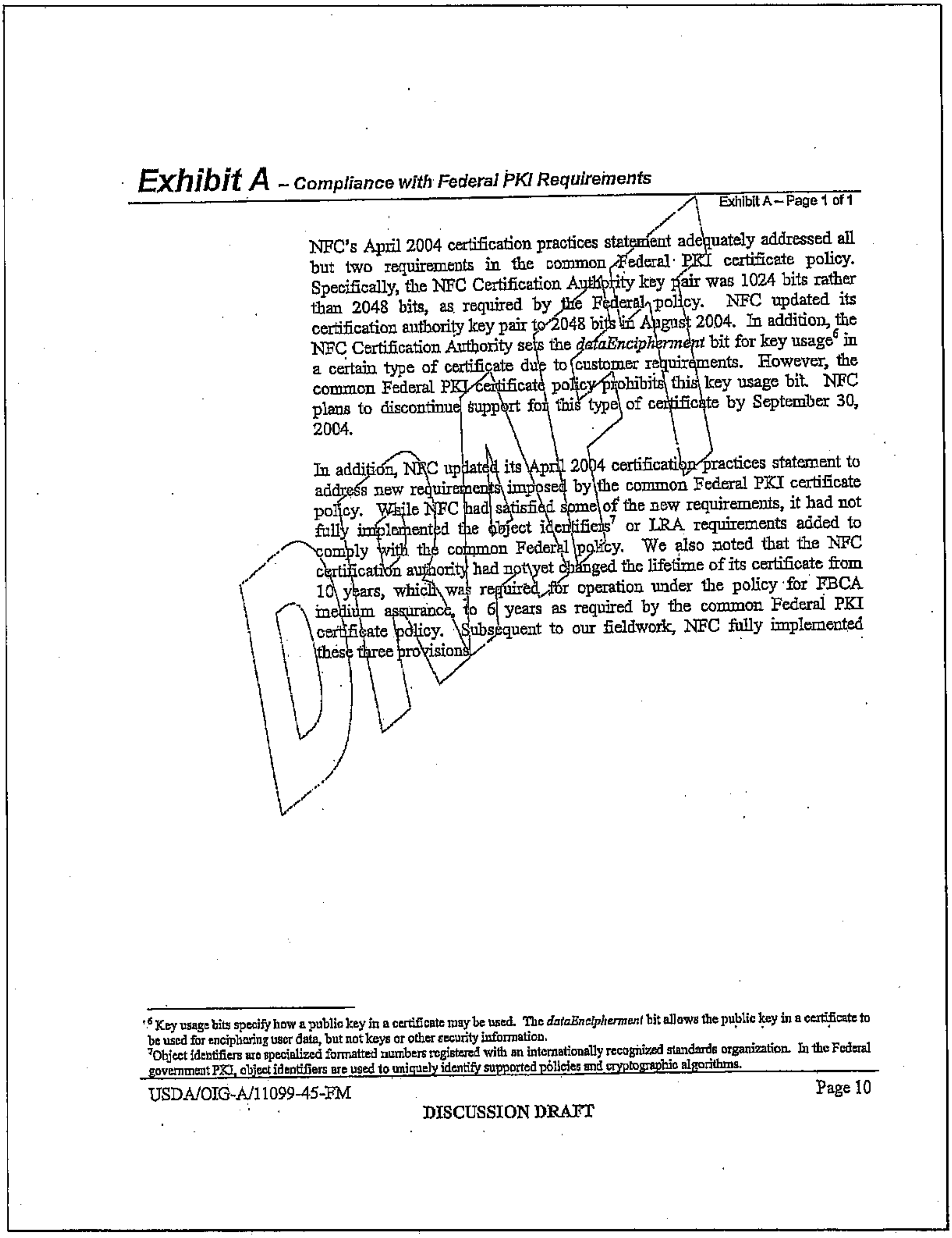
Management Response:

We agree with this recommendation. Testing plans, procedures and expected results are currently being documented, as well as the evaluation of the results of tests previously conducted.

Estimated Completion Date: November 30, 2004

Responsible Organization: ISPCS

Contact Person: Jim Julian, Chief, ISPCS (504) 426-0400.



NFC's April 2004 certification practices statement adequately addressed all but two requirements in the common Federal PKI certificate policy. Specifically, the NFC Certification Authority key pair was 1024 bits rather than 2048 bits, as required by the Federal policy. NFC updated its certification authority key pair to 2048 bits in August 2004. In addition, the NFC Certification Authority sets the *dataEncipherment* bit for key usage[6] in a certain type of certificate due to customer requirements. However, the common Federal PKI certificate policy prohibits this key usage bit. NFC plans to discontinue support for this type of certificate by September 30, 2004.

In addition, NFC updated its April 2004 certification practices statement to address new requirements imposed by the common Federal PKI certificate policy. While NFC had satisfied some of the new requirements, it had not fully implemented the object identifiers[7] or LRA requirements added to comply with the common Federal policy. We also noted that the NFC certification authority had not yet changed the lifetime of its certificate from 10 years, which was required for operation under the policy for FBCA medium assurance, to 6 years as required by the common Federal PKI certificate policy. Subsequent to our fieldwork, NFC fully implemented these three provisions.

[6] Key usage bits specify how a public key in a certificate may be used. The *dataEncipherment* bit allows the public key in a certificate to be used for enciphering user data, but not keys or other security information.

[7] Object identifiers are specialized formatted numbers registered with an internationally recognized standards organization. In the Federal government PKI, object identifiers are used to uniquely identify supported policies and cryptographic algorithms.

Glossary of Terms

Archive

Archives are databases of information maintained to settle future disputes. The archive includes information needed to determine if a digital signature on an old document should be trusted.

Certificate

A certificate is a digital representation of information that, at a minimum, (1) identifies and is digitally signed by the certification authority issuing it; (2) specifies the person, process, or equipment that is the user of the certificate; (3) contains the subscriber's public key; and (4) indicates the certificate's operational period.

Certificate Lifecycle

The user certificate lifecycle includes (1) the identification and authentication process that binds the individual subscriber to a certificate; (2) the renewal, rekey, revocation, and/or suspension of a certificate; and (3) the timely publication of certificate status information.

Certificate Policy

A certificate policy sets forth the general requirements for PKI participants and describes the appropriate uses for certificates. It provides the criteria that can be used by others to determine whether to trust certificates issued under the certificate policy.

Certification Authority

A certification authority confirms the identities of parties sending and receiving electronic payments or other communications. This is accomplished through the issuance of digital certificates that typically include a public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the certification authority's own digital signature. In addition, the certificate may contain other information about the signing party (e.g. certification authority) or information about the recommended uses for the public key.

Certification Practices Statement

A certification practices statement is typically a comprehensive statement of practices and procedures that a certification authority employs in issuing, suspending, revoking, and renewing digital certificates and providing access to them. Where a certificate policy sets forth general requirements, a certification practices statement explains how a certification authority meets the requirements of its certificate policy.

Key Compromise

Key compromise occurs when information is disclosed to unauthorized persons, either intentionally or unintentionally, or a security violation occurs that may lead to the inappropriate use, modification, loss, or destruction of an object—in this case a subscriber's key pair.

Key Management

Key management covers the generation, storage, backup, recovery, distribution, usage, destruction, and archival of certification authority cryptographic keys and the management of the cryptographic hardware used by the certification authority. Strong key life cycle management controls are vital to guard against key compromise that can damage the integrity of the pubic key infrastructure.

Key Pair

A key pair includes two mathematically related keys where (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key. The NFC PKI issues both encryption and signing key pairs. An encryption key pair consists of a encryption public key and a decryption private key. The public key portion of an encryption key pair is used to encrypt data that can be decrypted by the matching decryption private key. A signing key pair consists of a signing private key and a verification public key. The public key portion of a signing key pair is used to verify data that has been signed by the matching signing private key.

Key Recovery

Key recovery may be required when users forget passwords or their digital certificates are lost or damaged. In the NFC PKI, key recovery involves the re-issuance of the user's current encryption key pair and the generation of a new signing key pair for the user.

Key Usage

Key usage bits specify how a public key in a certificate may be used. The *dataEncipherment* bit allows the public key in a certificate to be used for enciphering user data, but not keys or other security information

Object Identifier

Object identifiers are specialized formatted numbers registered with an internationally recognized standards organization. In the Federal Government PKI, object identifiers are used to uniquely identify supported policies and cryptographic algorithms.

Private Key

A private key is (1) the key of a signature key pair used to create a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. In both cases, this key must be kept secret.

Public Key

A public key is (1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.

Public Key Cryptography

Public key cryptography, also known as asymmetric key cryptography, uses a class of algorithms that generate public and private key pairs in a manner that ensures that data encrypted with one key can be decrypted with the other key.

Public Key Infrastructure

PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks.

Registration Authority

A registration authority is an entity that is trusted by the certification authority to register or vouch for the identity of users to the certification authority.

Relying Party

A relying party uses PKI components to verify certificates of other entities and to know, with certainty, the public key of another subscriber.

Repository

A repository is a database of active digital certificates for certification authority systems. The repository allows relying parties to confirm the status of digital certificates when they receive digitally signed messages.

Subscriber

A subscriber is an individual or business entity that has contracted with a certification authority to receive a digital certificate that verifies its identity.

Informational copies of this report have been distributed to:

Agency Liaison Officer
General Accounting Office (1)
Office of Management and Budget (1)
Office of the Chief Financial Officer
Director, Planning and Accountability Division (1)

OIG Headquarters
  Director, AFD (2)
  OIG File Copy (1)
RIG, F&ADPO (1)