CRYPTOGRAPHIC INFRASTRUCTURE DESIGN

Audit Report No. 99-016
March 19, 1999

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

DATE: March 19, 1999

TO: Donald C. Demitros, Director
Division of Information Resources Management

FROM: David H. Loewenstein
Assistant Inspector General

SUBJECT: *Cryptographic Infrastructure Design*
(Audit Report No. 99-016)

The Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) has completed an audit of the design and implementation of computer-based cryptography for sensitive and critical corporate data. This was the second of two audits addressing the Corporation's planned use of cryptography.

Our first audit report, *Implementation of Electronic Signatures to Support the Electronic Travel Voucher Payment System (ETVPS) and Other Planned Applications* (Audit Report Number 98-052), was issued on June 30, 1998. That report focused on planning and management for providing encryption and digital signature technology in support of FDIC systems and data and contained three recommendations for improvements in the FDIC's methodology for developing its electronic signature infrastructure. We recommended that the FDIC develop a long-range plan and system architecture to bring the FDIC's electronic signature approach into full compliance with government-wide standards and U.S. General Accounting Office (GAO) requirements. We also recommended that the FDIC perform an alternatives and cost/benefit analysis comparing available alternatives for satisfying the FDIC's electronic signature needs. In addition, we recommended that the FDIC ensure that all Division of Information Resources Management (DIRM) security and program managers communicate on a regular basis to share pertinent information. DIRM provided a response indicating that it would address the recommendations and provided documentation during this audit demonstrating its efforts, thus far, to do so. This audit focused on DIRM's continued planning and management efforts related to encryption and electronic signature issues and its implementation of this technology for low- and moderate-risk application systems.

BACKGROUND

The FDIC is currently developing several major automated systems intended to reduce costs and paperwork. These systems are being designed to use cryptography for secure transmission and electronic approval of documents for payment or authorization purposes. Two recently developed applications designed to make use of cryptography are the Performance Reports On-Line System (PROS) and ETVPS.

Cryptography is the process of writing in or interpreting secret code. Effective use of public key cryptography provides the ability to securely exchange information with only selected recipients. A Public Key Infrastructure (PKI)[1] is the implementation of public key cryptography using computer hardware and software to establish trusted information-sharing among a select group of people. This framework includes the use of electronic credentials, often called digital certificates, and the management of public and private keys[2] needed to encode and electronically sign data and to decode and verify the integrity of electronically signed data produced by others. With electronically signed data, the recipient is assured of the signer's identity and that the signed data have not been altered.

The FDIC is currently using cryptography in two recently developed applications. The first, PROS, is an application designed to disseminate uniform bank, bank holding company, and uniform thrift performance reports to Division of Supervision and state bank examiners through the FDIC Intranet and the Internet, respectively. Additionally, ETVPS is a client server[3]-based application designed to provide a paperless method of handling travel arrangements and expense reimbursements.

The FDIC acquired and is implementing ENTRUST, a software product, to support its initial implementation of PKI technology for low- to moderate-risk applications such as ETVPS.

The National Institute of Standards and Technology (NIST) has a core mission of promoting economic growth by working with industry to develop technology, measurements, and standards. NIST has taken a leadership role in the development of standards for federal PKI that support electronic signatures and encryption services. One of NIST's primary roles in this capacity is coordinating the *Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules* validation program**.** NIST performed a cryptographic module validation (CMV) of the ENTRUST cryptographic module (CM) and assigned it a level-one rating when operating in FIPS-mode, the mode tested by NIST. Such a rating is the lowest on a scale of 1 to 4 and indicates that ENTRUST CM will provide security suitable for use within a security system supporting low- to moderate-risk applications. However, this rating only applies when the CM is operating on a single workstation, in single-user mode, under a Microsoft Windows operating system.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine the adequacy of controls supporting the FDIC's (1) encryption and authentication of data transmitted during an active session on an unsecured external telecommunications network and (2) implementation of hardware and software to provide initial encryption and electronic signature capabilities to support planned low- to moderate-risk paperless application systems. To accomplish our audit objectives, we reviewed

[1] A set of policies, procedures, hardware, and software used to manage the public/private key pairs to provide the ability to digitally sign or verify signed documents and encrypt or decrypt data.

[2] A numeric value that, along with a cryptographic algorithm, can encrypt, decrypt, sign, and verify data.

[3] A computer system characterized by an information technology architecture where software is distributed to both a user workstation and a network server for coordinated execution.

DIRM's conceptual design for providing encryption and PKI services, documentation related to security features of hardware and software supporting the implementation of encryption and electronic signature technologies, and other related documentation. We also interviewed DIRM personnel, ENTRUST manufacturer representatives, ENTRUST User Group representatives, and officials from NIST and GAO. We conducted the audit between April 1997 and November 1998 in accordance with generally accepted government auditing standards.

The scope of this audit was limited to an evaluation of DIRM's (1) deployment of secure-sockets-layer (SSL)[4] software to secure access to PROS; (2) deployment of ENTRUST to establish an initial PKI to support ETVPS; and (3) compliance with NIST and GAO requirements for carrying out these actions.

RESULTS OF AUDIT

DIRM implemented sufficient controls to support the use of SSL with PROS. Further, DIRM implemented some of the controls needed to support use of the ENTRUST manager, admin, and client components as the backbone of the FDIC PKI for low- to moderate-risk business applications. However, DIRM's system qualification testing (SQT) to ensure that functional requirements were satisfied was incomplete. Further, DIRM did not ensure adequate separation of duties for sensitive operations by employing ENTRUST's multiple authorization feature. In addition, security for the FDIC's PKI operations was reduced because the database that stores authenticated public-key certificates and the certificate authority that assures the authenticity of a digital certificate were operating from the same hardware platform in conflict with GAO requirements, which call for separate platforms. Finally, PKI internal control practices were not fully documented, and the FDIC's automated registration process for ENTRUST allowed the possibility for users to masquerade as other users.

DIRM demonstrated its intent to institute corrective actions in response to our recommendations throughout the audit. For example, during our review of the use of SSL with PROS, DIRM expanded its testing and tightened access privileges to sensitive files. Further, DIRM expanded its PROS security documentation to describe how a router was being used to prevent unauthorized access from the Internet. In addition, DIRM substantially improved its ENTRUST security and control documentation in response to our observations and suggestions. For example, DIRM established a PKI Concept of Operations, documenting its plans for implementing and operating its PKI operations, and developed an ENTRUST Installation Document. DIRM also enhanced its PKI policies and procedures related to low- and moderate-risk applications. Finally, DIRM committed to enhancing future controls by implementing a FIPS 140-1 level-three-compliant hardware certificate authority to establish a single PKI to support the FDIC's high-, medium-, and low-risk business applications.

Appendix I contains more detail on some specific conditions noted during this audit. These conditions are generally described in the following sections of this report, and more details are

[4] An industry standard software-based protocol designed to provide privacy during telecommunications between two sites using cryptography.

presented in appendix I due to their technical nature.

ENTRUST SYSTEM QUALIFICATION TESTING COULD BE IMPROVED

DIRM Security had not performed thorough and complete SQT for ENTRUST. DIRM Security officials indicated that SQT for ENTRUST was not necessary because the ENTRUST cryptographic module had undergone NIST accreditation for conformance to *FIPS 140-1 Security Requirements for Cryptographic Modules*. Thorough and complete SQT is needed to ensure that a system is functioning as intended and provides adequate security and controls.

We confirmed that NIST had performed FIPS 140-1 cryptographic module validation (CMV) testing for ENTRUST's cryptographic module component. However, NIST's CMV testing does not impact the FDIC's need to test ENTRUST implementation in its actual operating environment. NIST testing for ENTRUST was conducted in a laboratory setting with the cryptographic module running on a single, non-networked microcomputer operating in single-user mode under Microsoft Windows operating systems. By contrast, the FDIC operates a series of local area networks connected by a wide area network and intends to use ENTRUST in a multi-user mode. In addition, we noted that the NIST testing was not applied to all features of ENTRUST, and the operating system tested differed from the Sun Solaris operating system used by the FDIC.

The FDIC's system development life cycle methodology requires SQT for all software development and acquisition activities to ensure that functional requirements have been addressed. Prudent information resources management dictates thorough testing of any complex process involving new information technology such as a PKI. Also, cryptographic algorithms, the formulas that provide the basis for encryption used by the U.S. Government, must be sanctioned by NIST and are currently limited to three specific algorithms. Accordingly, ENTRUST system users should not be provided the option of selecting cryptographic algorithms that may not be compliant with NIST standards. Finally, any cryptographic modules used by the U.S. Government for conducting official business must conform to *FIPS 140-1 Security Requirements for Cryptographic Modules* as well as GAO requirements.

Several major ENTRUST control features were not supported by evidence of SQT. Ineffective operation of these control features could expose the FDIC's related processes, data, and systems to increased risk of inappropriate and undetected activity. Specific examples of the major ENTRUST control features that were not thoroughly and completely tested are listed in appendix I.

We identified four causes for DIRM's incomplete testing of ENTRUST. First, DIRM Security officials interpreted the FIPS 140-1 CMV testing as being an all-inclusive substitute for in-house SQT. Second, the ENTRUST design feature that permits users to select the encryption algorithms to be employed is subtle and can be overlooked. Third, ENTRUST operation in non-FIPS mode is a system default and the use of this system default was a design decision to facilitate the use of ENTRUST with certain cryptographic hardware devices that require keys to be loaded in clear text. Finally, DIRM Security's evaluation and testing of ENTRUST software

did not identify encryption-option-method-selection and operating-in-non-FIPS-mode design features as potential control issues.

The effect of an incomplete ENTRUST SQT is that the implemented PKI may not function as intended by management. As discussed earlier, the FDIC's planned implementation of ENTRUST permitted users to select the cryptographic algorithm to be used. Such an option may result in FDIC users employing algorithms not sanctioned by NIST to encrypt sensitive corporate data. Consequently, sensitive corporate data may be subject to unauthorized disclosure because cryptographic algorithms selected may be weaker than NIST-sanctioned algorithms. ENTRUST can be operated from either FIPS mode or non-FIPS mode. Operating ENTRUST in non-FIPS mode voids NIST sanctioning and reduces controls. The resultant reduction in controls could result in corruption of the cryptographic module, including the certificates issued, and provide the ability to export private cryptographic keys in clear text that has not been encrypted.

After discussing these conditions with DIRM officials, DIRM agreed to perform and document testing of the PKI control features discussed above, expanded the project schedule to include additional testing, and provided us with a copy of the revised schedule.

Recommendations

We recommend that the Director, DIRM, continue to:

(1) Ensure that SQT of major PKI control features of and related to ENTRUST are performed and documented to supplement the FIPS 140-1 CMV testing.
(2) Enforce the use of only NIST-sanctioned cryptographic algorithms through ENTRUST for encrypting sensitive corporate data.
(3) Prevent system users from being able to choose the cryptographic algorithm to be used for encrypting sensitive corporate data.
(4) Ensure that the version of ENTRUST used at the FDIC operates in FIPS mode.

ENTRUST MULTIPLE AUTHORIZATION FEATURE NOT IN USE

DIRM missed an opportunity to better control the integrity of its planned PKI operations. ENTRUST's multiple authorization feature (MAF) can require the involvement of at least two individuals to perform and authorize sensitive PKI operations. However, DIRM had not implemented this control. Instead, this capability was set so that only one individual was required to perform and authorize sensitive PKI operations. Sensitive PKI operations include enabling and disabling ENTRUST security officers, administrators, and directory administrators; setting default lifetimes for user cryptographic keys, certificate revocation lists, and cross-certificates; and cross-certifying with other certificate authorities.

Prudent PKI management requires the use of system-enforced dual control over sensitive PKI operations. The manufacturer of ENTRUST recommends that multiple authorizations be used for sensitive PKI operations. Furthermore, GAO requirements specify the need for dual control within PKI operations.

DIRM officials stated that the MAF was set to permit one person to perform these sensitive operations for operational efficiency. Further, even though the manufacturer recommends multiple authorizations for sensitive operations, ENTRUST's default setting for this function is set to one and requires modification to provide the recommended security.

A MAF setting of one provides an administrator or security officer the ability to gain access to a user's ENTRUST identity without the knowledge of at least one other administrator or security officer. In such an environment, the administrator or security officer can perform sensitive functions such as establishing the useful life for keys, certificates, and revocation lists. A key is a numeric value that, along with a cryptographic algorithm, can encrypt, decrypt, sign and, verify data. A certificate is a tamperproof set of data assigned to an individual for use in the encryption process. A revocation list is an electronically signed list of revoked certificates. The lifetime established for these entities determines their strength as a control feature. For example, the shorter a private key's lifetime, the greater the probability of it not being discovered by unauthorized parties.

Recommendation

We recommend that the Director, DIRM, ensure that:

(5) The ENTRUST multiple authorization feature be set to a minimum of two so that all sensitive PKI operations require the involvement of at least two individuals.

THE FDIC's X500 DIRECTORY AND CERTIFICATE AUTHORITY WERE OPERATING FROM THE SAME PLATFORM

DIRM's installation of two major components of the PKI on one workstation reduced security over DIRM's operations. A single workstation contained both the X500 directory, used to store the public keys assigned to users to ensure secure communications, and the certificate authority (CA) component of ENTRUST that verifies the authenticity of digital certificates created by users. GAO requires that the X500 directory and CA reside on separate hardware platforms to preclude unnecessary network access to the CA. The manufacturer of ENTRUST also recommends that the X500 directory reside on a separate hardware platform from the one housing other ENTRUST software components to improve security.

DIRM stored the X500 directory and other ENTRUST components on the same hardware platform to enhance operational convenience and network performance. In fact, the manufacturer had recommended, for earlier versions of the software, that the X500 directory reside on the same hardware platform as the other ENTRUST components.

Frequent network access to the hardware platform to obtain certificates from the X500 directory increases the risk of unauthorized access and compromise to the CA due to potential malfunction of operating-system-level software that governs access control. Storing the CA on a separate platform significantly reduces such an exposure.

Recommendation

We recommend that the Director, DIRM:

(6) Require operation of the FDIC X500 directory and CA from separate hardware platforms.

PKI INTERNAL CONTROL PRACTICES NOT FULLY DOCUMENTED

DIRM made substantial progress in establishing control practice documentation during our audit. In response to an OIG recommendation contained in our earlier audit report (98-052), DIRM established a PKI Concept of Operations. Based upon proposed recommendations during our current audit, DIRM established an ENTRUST Installation Document and enhanced its Low-to-Moderate Assurance Certification Policy and Practices Statement. However, documentation describing the control practices used in operating and managing the PKI remained incomplete. Missing or incomplete documentation included that related to access controls and other security features, configuration management to control changes to the software, DIRM's registration process for assigning digital certificates to users, and descriptions of files used by the software-based CA. See appendix I for a more detailed listing of the missing or incomplete documentation.

A PKI must be thoroughly documented to ensure understanding by management, administration, and user personnel; consistency with management's intentions; and conformance to prudent control practices. However, documentation preparation often receives lower priority than other design and implementation tasks. Because of the importance of this new technology and its potential impact on corporate operations, it is critical that the implemented PKI be understood, consistent with management's intentions, and adequately controlled.

DIRM agreed to develop the needed additional PKI control practice documentation that we identified. DIRM expanded its project schedule to include such documentation requirements and provided us with a copy of the revised schedule.

Recommendation

We recommend that the Director, DIRM:

(7) Continue to require that complete and accurate documentation describing the control practices used in operating and managing the FDIC PKI be established and maintained.

AUTOMATED REGISTRATION PROCESS INCREASED OPPORTUNITIES FOR MASQUERADING

When users want to use their electronic identity, it is important that the system first validate that identity. DIRM's conceptual design for ENTRUST's automated registration process, however, contained a limitation that could result in electronic identity compromise. Specifically, the

potential exists for one system user to disguise himself or herself as another system user and be registered to use ENTRUST as that other user. The masquerade could continue until the legitimate user attempts the ENTRUST registration process.

Such "masquerading" could occur because the proposed automated ENTRUST registration process did not link the social security number of the registering user with the Windows-NT login process. The Windows NT login process is the validation of a user's identity before permitting access to the FDIC's local and wide area networks. DIRM planned to register users under ENTRUST by having them enter their social security number during the registration process following successful NT access but without precluding them from entering the social security number of another. This process could increase the FDIC's exposure to masquerading because of the availability of user social security numbers within the FDIC, including their display on hardcopy documents such as time sheets, leave slips, and training forms.

The effect of this condition is twofold. First, successful ENTRUST automated registration process masquerading would permit a masquerader to assume another's identity and send encrypted or signed information to other users. A masquerader would also be able to accept and use encrypted and signed information sent by others to the legitimate user whose identity the masquerader has assumed. Second, masquerading, regardless of duration, may permit inappropriate use of impacted business applications such as the ETVPS. In other words, travel information may be falsified or improperly approved and could result in fraudulent claims for reimbursement.

DIRM agreed that this condition warranted corrective action and has agreed to modify the automated registration process design to restrict a user from employing the social security number of another user to achieve successful ENTRUST registration. We, therefore, are not making any formal recommendations related to this condition.

CORPORATION COMMENTS AND OIG EVALUATION

On March 4, 1999, the Director, DIRM, provided a written response to the draft report. The response is presented in Appendix II of this report. The Director, DIRM, stated that he will complete actions to address the report's findings by August 31, 1999.

The Corporation's response to the draft report provided the elements necessary for management decisions on the report's recommendations. Therefore, no further response to this report is necessary. Appendix III presents management's proposed action on our recommendations and shows that there is a management decision for each recommendation in this report.

DETAILS OF CONDITIONS

ENTRUST System Qualification Testing Could Be Improved in the Following Areas:

- Secure Exchange Protocol and ENTRUST Session use to secure communication among the ENTRUST manager, administration, and client components.
- Sun Solaris ENTRUST platform password and other operating system level security features.
- Non-FIPS mode operating parameter of ENTRUST. When operating in this mode, NIST accreditation of the ENTRUST cryptographic module is nullified.
- Encryption method option of ENTRUST. This option permits system users to select cryptographic algorithms for encrypting sensitive corporate data that are not NIST-sanctioned.
- ENTRUST network performance.

PKI Internal Control Practices Not Fully Documented

- ENTRUST installation and customization documentation, in terms of (1) the International Computers Limited's (ICL) X500 directory operational attribute settings governing access control and shadowing, (2) Sun Solaris operating system security features used, and (3) ENTRUST security policy configuration, or simply stated, the use of ENTRUST features to achieve the FDIC's security objectives was incomplete.
- ENTRUST and SCM software configuration management practices documentation was limited to the build process employed for all multi-tiered application architecture common objects. Software configuration management is an umbrella activity that controls the application of changes to software.
- Secure Communication Manager (a software component of the FDIC Multi-Tier Application Manager Architecture that provides encryption and electronic signature services to business applications) test documentation was incomplete.
- Automated ENTRUST registration process (procedures followed to validate a user's identity as a prerequisite to assigning them an electronic identity such as a digital certificate) documentation was limited to a six-page draft of system qualification test requirements, prerequisites, and scripts document.
- High assurance certificate policy and practice statements were not yet available.
- ENTRUST Manager file descriptions were incomplete in terms of the purpose of binary files and their relationship to the software-based CA.

APPENDIX II

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
3501 North Fairfax Drive. Arlington, VA 22226 Division of Information Resources Management

March 4, 1999

MEMORANDUM TO: David H. Loewenstein
Assistant Inspector General

FROM: Donald C. Demitros, Director
Division of Information Resources Management

SUBJECT: DIRM Management Response to the Draft OIG Report Entitled, *Cryptographic Infrastructure Design (CID) Audit* (Audit Number 97-902)

The Division of Information Resources Management (DIRM) has reviewed the draft audit report and, in general, agrees with the findings and recommendations.

We would like to thank the OIG staff for working so closely with the DIRM ISS staff during the preparation of this report. The recommendations of the OIG on this audit has enabled DIRM to identify and implement a number of corrective actions to date. Examples include DIRM's expansion of testing and tightening of access privileges to sensitive files associated with the Performance Reports On-line System (PROS) during the review of the secure-sockets-layer (SSL) software; expansion of PROS security documentation; and improved ENTRUST security and control documentation including Public Key Infrastructure (PKI) Concepts of Operation and ENTRUST Installation documents. PKI policies and procedures were also enhanced relative to low and moderate risk applications.

Each of the conditions and recommendations from the draft report are identified below. DIRM's management response including any corrective action is provided immediately following each specific recommendation.

APPENDIX II

CORPORATION COMMENTS

ENTRUST SYSTEM QUALIFICATION TESTING COULD BE IMPROVED

Recommendations

We recommend that the Director, DIRM, continue to:

(1) Ensure that SQT of major PKI control features of and related to ENTRUST are performed and documented to supplement the FIPS 140-1 CMV testing.

Corrective Action: The Information Security Staff (ISS) is developing a comprehensive set of test plans to fully test all aspects of the FDIC PKI. The former virus test lab has been modified to accommodate PKI component testing. Expected completion of the testing is 6/30/99.

(2) Enforce the use of only NIST-sanctioned cryptographic algorithms through ENTRUST for encrypting sensitive corporate data.

Management Response: DIRM Security Policy 98-012, FDIC Encryption/Digital Signature and Public Key Infrastructure (PKI) Standard published 9/29/98 states that ENTRUST hardware and software is the corporate standard for encryption/digital signature and Public Key Infrastructure (PKI). FDIC applications that use ENTRUST will make use of NIST-sanctioned algorithms and those algorithms will be provided as the initial default selection.

(3) Prevent system users from being able to choose the cryptographic algorithm to be used for encrypting sensitive corporate data.

Corrective Action: FDIC organizations have a business need for secure communications within the corporation and with external business partners including commercial firms, state bank examiners, etc. By 8/31/1999, DIRM will prepare a policy memorandum specifying the cryptographic algorithm to be used for secure internal communications and will provide this algorithm as the initial default when deploying ENTRUST. Because of the need for secure external communications that must use the cryptographic algorithm selected by our business partners, the ability to select other than the initial default algorithm must also be made available. DIRM staff, in conjunction with OIG staff, will work to identify technical alternatives to this current procedure. If OIG can commit resources, DIRM proposes to conduct this identification of technical alternatives, if any, by 6/30/99.

(4) Ensure that the version of ENTRUST used at the FDIC operates in FIPS mode.

Corrective Action: A revised entrust.ini file which will change the ENTRUST version used at the FDIC so that it will operate in FIPS mode will be distributed following testing by DIRM ISS Operations. Estimated completion date 8/31/99.

APPENDIX II

CORPORATION COMMENTS

ENTRUST MULTIPLE AUTHORIZATION FEATURE NOT IN USE

Recommendation

We recommend that the Director, DIRM, ensure that:

(5) The ENTRUST multiple authorization feature be set to a minimum of two so that all sensitive PKI operations require the involvement of at least two individuals.

Corrective Action: The ENTRUST multiple authorization feature can currently be set to a minimum of two for some sensitive PKI operations. DIRM is setting this feature at a minimum of two for select actions by Security Officers. In addition, DIRM will set this feature for the Entrust Manager, which currently uses a software implementation that is specific to three Master Users. DIRM is in the process of identifying and obtaining necessary hardware required to support all remaining sensitive PKI operations. ISS is currently obtaining Level 3 – 4 hardware cryptographic modules for lab testing with our PKI. The conversion to a hardware cryptographic module is predicated on the conversion of the Entrust Manager from its current version (3.0c1) to version 4.X running on a Windows NT server. A cost benefit analysis was conducted showing the importance of maintaining the initial approach of converting from Unix to Windows NT. Estimated completion date for enabling the multiple authorization feature for select Security Officers and Entrust Manager actions is 6/30/99. The estimated completion date for obtaining and implementing the necessary hardware and setting the multiple authorization feature on the remaining sensitive PKI operations is 8/31/99.

THE FDIC's X500 DIRECTORY AND CERTIFICATE AUTHORITY WERE OPERATING FROM THE SAME PLATFORM

Recommendation

We recommend that the Director, DIRM:

(6) Require operation of the FDIC X500 directory and CA from separate hardware platforms.

Corrective Action: DIRM is developing procedures and guidance to require operation of the FDIC X500 directory and CA from separate hardware platforms. Current estimated completion date is 8/31/99.

APPENDIX II

CORPORATION COMMENTS

PKI INTERNAL CONTROL PRACTICES NOT FULLY DOCUMENTED

Recommendation

We recommend that the Director, DIRM:

(7) Continue to require that complete and accurate documentation describing the control practices used in operating and managing the FDIC PKI be established and maintained.

> **Corrective Action:** DIRM ISS is in the process of updating and validating all test, operation, and recovery procedures and documentation. OIG personnel will be provided documentation as it is prepared. Estimated completion is 6/30/99.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on 516-1422.

cc: Robert M. Cittadino, OICM
Howard Furner, OICM

MANAGEMENT RESPONSES TO RECOMMENDATIONS

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC's responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management's response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid.
Second, the OIG must determine that management's descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management's written response to our report and subsequent discussions with management representatives.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	The Corporation agreed with the recommendation. DIRM will perform the recommended testing of major PKI control features.	June 30, 1999	DIRM documented test results	None	Yes
2	The Corporation agreed with the recommendation. DIRM will issue a policy memorandum specifiying that FDIC applications will use NIST sanctioned algorithms. Such algorithms will also be provided as the initial default selection.	August 31, 1999	DIRM policy memorandum and system specifications	None	Yes
3	The Corporation agreed with the recommendation. DIRM will issue a policy memorandum specifying the cryptographic algorithms to be used for internal communications and will provide this algorithm as the initial default when deploying ENTRUST. DIRM will also perform an analysis to identify alternative methods for controlled use of other algorithms to facilitate secure external communication with selected business partners.	August 31, 1999	DIRM policy memorandum and alternatives analysis	None	Yes
4	The Corporation agreed with the recommendation. DIRM will test and distribute a revised entrust.ini file that will ensure that the ENTRUST software operates in FIPS mode.	August 31, 1999	DIRM documented test results and software distribution records	None	Yes
5	The Corporation agreed with the recommendation. DIRM will change the ENTRUST multiple authorization feature so that more than one individual is involved with all sensitive PKI operations.	August 31, 1999	DIRM system specifications supporting the ENTRUST multiple authorization feature	None	Yes
6	The Corporation agreed with the recommendation. DIRM will operate the X500 directory and certificate authority from separate hardware platforms.	August 31, 1999	DIRM PKI system configuration documentation	None	Yes
7	The Corporation agreed with the recommendation. DIRM will establish complete and accurate control practice documentation for PKI operation and management.	June 30, 1999	DIRM PKI control practice documentation	None	Yes