Audit of FDIC's Public Key Infrastructure Certificate Policy and Extranet Certification Practice Statement

(Report No. 04-024, July 2, 2004)

Summary

PKI is a set of policies, processes, hardware, and software that enables secure and private communication. The Certificate Policy (CP) defines the high-level PKI standards and requirements and the Certification Practice Statement (CPS) describes the detailed practices that implement the CP. The Federal Bridge Certification Authority (FBCA), which became operational in June 2001, provides the technical infrastructure, and appropriate security policies and procedures to ensure that members follow common PKI security practices in order to cross-certify with the FBCA. As a pre-requisite for cross-certification with the FBCA, applicant organizations are required to engage a qualified independent third party to perform a compliance audit of their CP and CPS.

This audit was requested by the former Acting Director, Division of Information Resources Management (DIRM), in support of the FDIC's ongoing effort to cross-certify its Extranet PKI Service with the FBCA. The objective of the audit was to determine whether (1) the FDIC's Certificate Policy complies with the requirements defined in the FBCA's Certificate Policy for achieving the basic level of assurance and (2) the Extranet Certification Practice Statement is consistent with the FDIC's Certificate Policy.

The OIG concluded that in general, the FDIC's Certificate Policy complied with the requirements defined in the FBCA's Certificate Policy for achieving the basic level of assurance. However, we are recommending that DIRM take additional actions to improve the CP and CPS.

Recommendations

The OIG recommended DIRM clarify the Certification Practice Statement and performing quality assurance and legal sufficiency reviews of the PKI policy and practice statements to ensure that these documents accurately reflect the current environment and provide definitive guidance.

Management Response

DIRM's response adequately addresses the recommendations.

This report addresses issues associated with information security. Accordingly, we have not made, nor do we intend to make, public release of the specific contents of the report.