Private & Confidential

AUDIT OF CERTIFICATE AUTHORITY

Netrust Pte Ltd
Version 1.0

25 April 2010

Report By:

Tay Ghim Hui
Associate Security Consultant

Email : tay.ghimhui@e-cop.net
Fax : (65) 6788 3883

Review By:

Philip Sy
Principal Consultant

Email : Philip.sy@e-cop.net
Fax : (65) 6788 3883

e-Cop (S) Pte Ltd
23 Serangoon North Avenue 5
#06-01 BTH Centre
Singapore 554530

Table of Contents

1. Executive Summary

e-Cop (S) Pte Ltd hereafter known as e-Cop was contracted by Netrust Pte Ltd hereafter known as Netrust to carry out an independent third party information systems security Audit. The purpose of this audit was to express an opinion on the compliance of Netrust in implementing the control objectives as specified in the *Security Guidelines for Certificate Authority* and the *ISO27001/27002:2005 Standard.* The scope of this audit included an assessment of the policies, procedures, processes, systems and controls included in the *Security Guidelines for Certificate Authority by IDA.* The audit guide for this audit was also backed up by relevant industry best practices based on ISO 27002:2005.

The assessment date was from 26 March 2010 – 19 April 2010. The auditor team undertook a process of collecting and evaluating evidence to determine level of compliance.

Except for the findings mentioned in Section 4, Netrust was in all material respects, in compliance with the IDA Guidelines for Certificate Authority. We have provided recommendations in section 4.0 to address issues or areas for improvement identified during our audit.

The following areas were covered during the review:

- Management Guidelines (IDA Guidelines Section 2.0)
- Certificate Management (IDA Guidelines Section 3.0)
- Key Management (IDA Guidelines Section 4.0)
- Systems & Operations IDA Guidelines Section 5.0)
- Security Policy (ISO 27001/27002:2005 Section 5)
- Human resources security (ISO 27001/27002:2005 Section 8)
- Physical and environmental security (ISO 27001/27002:2005 Section 9)
- Business Continuity Planning (ISO 27001/27002:2005 Section 9)

Our opinion is that Netrust has implemented critical controls except for the findings described in *Section 4* as of 19 April 2010. Further we also acknowledge that Netrust is taking active corrective action to implement control measures to mitigate the potential risks that could result from the control deficiencies highlighted in our review.

e-Cop (S) Pte Ltd
23 Serangoon North Avenue 5
#06-01 BTH Centre
Singapore 554530

To: Mr Foo Jong Ai
Chief Executive Officer
Netrust Pte Ltd
70 Bendemeer Road
#05-03 Luzerne
Singapore 339940

SIGNOFF & ACKNOWLEDGMENT

e-Cop would like to take this opportunity to thank the Management and staff of **Netrust** for all their assistance and time during the course of this audit.

This report is intended solely for use by the Management of **Netrust** and e-Cop accept no responsibility for any reliance on the report by any third parties, unless our permission is sought for the provision of the particular report to specified third parties and such request is given to us in writing prior to provision of the report.

This acknowledgement represents the agreement between e-Cop and **Netrust** with respect to the objectives, obligations and responsibilities performed in the audit had been completed.

<u>Netrust contact:</u>

Accepted by:

....

Date: 17/5/10

<u>e-Cop Consultants:</u>

Prepared by:

Tay Ghim Hui,

Associate Security Consultant

....

Date: 17/5/10

Reviewed by:

Philip Sy

Principal Consultant

....

Date: 17/5/10

Please return or fax this copy to e-Cop.net at +65-6788.3883

If this form is not returned within five (5) days, e-Cop will assume full acceptance of this report without modification.

2. Background

2.1. Introduction

Netrust was established in May 1997 as the first Certification Authority ("CA") in Southeast Asia. Netrust provides individuals, businesses and government organisations with a complete online identification and security infrastructure to enable secure electronic transactions via the Internet and other wireless media.

In its capacity as a CA, Netrust acts as a trusted third party ("TTP") that issues and manages digital certificates. Netrust maintains a Public Key Infrastructure ("PKI") certification service and in its CA role creates and signs X.509 digital certificates which bind individuals, organisations and application servers with the particular public key of each subscriber.

Netrust's PKI provides a secure environment where faceless electronic transactions can take place with trust on the Internet, Intranet and on wireless networks. It issues to participants of this environment, digital certificates - which are equivalent to electronic IDs - that give online identities to individuals, organisations and application servers. Netrust's digital certificates can be issued globally and provide complete online identification and security for secure electronic transactions.

Netrust issues a range of digital certificates for online applications including secure access to government applications, Internet banking, supply chain management, virtual private networks and secure access to intranet portals. It supports the core Security Guidelines of Authentication, Authorization, Confidentiality, Data Integrity and Non-Repudiation.

The Electronic Transactions Act ("ETA") was enacted on 10 July 1998 to create a legal framework for electronic commerce transactions in Singapore. Following the ETA, the Electronic Transactions (Certification Authority) Regulations ("ETR") came into operation on 10 February 1999 to provide regulations for the licensing and regulation of certification authorities ("CAs") in Singapore. The Controller of Certification Authorities ("CCA") also published security guidelines in September 1999 to establish the security criteria for the management, systems and operations of CAs. The voluntary licensing programme aims to promote high integrity licensed CAs that can be trusted. The CCA awarded the CA License to Netrust in June 2001.

The ETR requires regular audits to be conducted on Netrust to provide assurance that the IT systems and processes of Netrust fulfill the requisite Security Guidelines, as set forth in the security guidelines issued by the CCA, as well as international standard such as the ISO 27001/27002:2005.

2.2. Objectives

The overall objectives of the review are to:

- Review the control procedures established by Netrust for compliance with the requirements set out in the "Security Guidelines for Certification Authorities (version 2.0)" issued by the Controller of Certification Authority from the Infocomm Development Authority ("IDA") of Singapore; and

- Ascertain whether Netrust has met the requirements set out in the Electronic Transactions Act 1998 ("ETA"), the Electronic Transactions (CA) Regulations 1999 ("ETR") and the ISO27002 (2005) Standard.

2.3. Scope and Approach

Our review work was performed from March 26, 2010 to April 19, 2010. Our report of the detailed findings and recommendations was discussed with appropriate management and staff at Netrust and finalised on May 13, 2010.

The scope of our work covered the IT systems and processes that are directly deployed in providing the CA services. To achieve the objectives of this review, we performed specific review procedures, as follows:

- Gained an understanding of the Netrust PKI/CA business model and trust required(s) in the CA through discussions with Netrust CA personnel, a review of technical and operations documentation, and a review of the CPS and CP(s);

- Reviewed the control procedures established by Netrust to ascertain compliance with the requirements set out in the IDA guidelines, ETA, ETR and ISO27001/17799:2005 Standard. Our review covered those practices and procedures that create a secure and trustworthy environment for the CA, as follows:

  CA Management Controls
  The components of primary CA management controls include:

  - Obligations;
  - Liability of the CA;
  - Certificate Policy and Certificate Practice Statement;
  - Security management;

- Risk management;
- Personnel security;
- Maintenance of subscribers' data;
- Incident management; and
- Business continuity planning.

Certificate Management Life Cycle Controls

The certificate life cycle covers the end-to-end process of certificate management and represents the core functions of a CA. The certificate life cycle controls include:

- Certificate attributes;
- Certificate registration;
- Certificate generation;
- Certificate issuance;
- Certificate publication/distribution;
- Certificate renewal;
- Certificate suspension;
- Certificate revocation (including CRL processing);
- Certificate archival; and
- Audit trails.

Key Management Life Cycle Controls

The key management life cycle controls is dependent on the strength of the primary CA controls. The key management life cycle controls include:

- Key generation;
- Key distribution;
- Key storage;
- Key usage;
- Key backup and recovery;
- Key change;
- Key destruction;
- Key compromise;
- Key archival; and
- Cryptographic Engineering.

Systems and Operations Controls
The components of systems and operations controls include:

- Physical security;
- Systems and software integrity and control;
- Change and configuration management;
- Network and communications security; and
- Monitoring and audit logs.

Application Integration Controls
We reviewed the security and control features/facilities of the toolkits provided by the CA to the user community to ensure secure implementation and operation. Our review excluded the application interfaces provided by the CA software vendor or the CA to the application developers. The components of application integration controls include:

- Integrity of signing and verification functions;
- Protection of private key;
- Verification of certificates.

Our review was based on interviews and discussions with key Netrust management and staff, and on a review of user documentation made available to us. In areas where independent corroboration was not available, written representations were obtained from Netrust.

3. Limitation or Our Work and Liability

3.1. Use of Our Report

This report has been prepared solely for the management of Netrust. We would not generally permit the use of our deliverables, or references to it, in material disseminated to the general public or third parties without our written permission, with the exception of the Infocomm Development of Singapore ("IDA").

3.2. Limitation of Controls

Control policies and procedures designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Therefore, constant monitoring is needed to ensure that system controls that exist remain effective over time.

3.3. Limitation of Liability

Netrust will indemnify and hold harmless e-Cop from claims, liabilities and costs to third parties where Netrust divulges any advice rendered by e-Cop pursuant to this engagement without e-Cop's consent to such parties and such third parties claim against e-Cop for losses suffered by them as a result of their reliance on such advice.

e-Cop will not be liable for any loss or damage caused by or arising from any fraudulent acts, misrepresentation, or willful default on the part of Netrust, its management, or employees.

4 Findings and Recommendations

IDA SGCA	ISO 27002:2005	Security Guidelines	Findings & Recommendations	Management Response

IDA SGCA	ISO 27002:2005	Security Guidelines	Findings & Recommendations	Management Response
2.5.3, 6.1.4	4.1	Risk management policies and procedures shall be reviewed periodically as part of a comprehensive risk management approach. (IDA SGCA) Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA software that manages, issues and revokes certificates is developed to manage the risk identified. (IDA SGCA) Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems. Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation). Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation. (ISO 27002)	**Issue:** it was observed that the risk management approach ,as laid down in the Risk Assessment Policy, did not contain the following elements which were essential: a. risk acceptance criteria; b. risk treatment process; and c. the frequency for the review of risk management approach. Moreover, the following issues were found in the risk assessment report v1.0 d/d Mar 2010: a. the calculation of risk value did not follow the methodology, e.g. item 2 and item 5; b. the risk scenario could be more comprehensive to cover relevant risks, e.g. malicious codes, remote system intrusion, certification key loss or compromise, and social engineering; c. there was no explicit risk treatment plan formulated to facilitate the implementation, follow-up and closure of risk treatment actions; and d. there were no committed dates for the risk treatment actions for follow-up and closure purpose. **Recommendation:** Include explicitly in the Risk Assessment Policy the risk acceptance criteria and risk treatment process, as well as the review frequency of the risk management approach. Ensure comprehensive coverage of risk scenario, accurate calculation of risk value, and effective follow-up.	We will review and update our Risk Assessment Policy to include Risk Acceptance Criteria and Risk Treatment Process as well as the review frequency.

IDA SGCA	ISO 27002:2005	Security Guidelines	Findings & Recommendations	Management Response
2.6.6, 2.6.7	6.1.3, 8.2.2	Dual control and segregation of duties shall be implemented for critical CA services and processes. In particular, technical personnel involved in critical CA services and processes such as the CA system administrators and operators shall not be given security related roles. Security related roles shall be given to dedicated personnel who are adequately trained to perform the job without any conflict of interest.	**Issue:** At the time of audit, the F&A Manager took up the role of Security Officer. However the following issues were identified: a. it was observed that the role and responsibility of Security Officer were dispersed through different plans and procedures. There was no consolidated role and responsibilities spelt out for the role of Security Officer; and b. at the time of audit, there was no evidence that the Security Officer continued to receive training to enable him to carry out his role. **Recommendation:** Document explicit, consolidated and comprehensive roles and responsibilities for security related roles including Security Officer. Furthermore, ensure that the security related roles, especially the Security Officer, continue to receive appropriate training to enable him to carry out his work.	The roles and responsibilities of Security Officer would be consolidated so as to better facilitate the functions of the Security Officer. We will look into the training of Security Officer.
		Security Officer shall also review the CD, CM, firewall & biometric logs regularly (CA Operations Manual)	**Issue:** Currently operations manager is the one reviewing the security logs and it does not comply to the policy. **Recommendation:** Netrust should appoint a security officer to reviewing the logs	The Security Officer will be reviewing the security logs periodically.

IDA SGCA	ISO 27002:2005	Security Guidelines	Findings & Recommendations	Management Response
2.9.4	10.5.1		**Issue:** There was a review of the backup tapes however it does not show who is the person doing the testing and it does not show the review was verified by a manager **Recommendation:** The person doing the testing should be include their names on the checklist and a manager should verified that the review was done properly.	The review did show who is doing the testing. We will ensure that the review will be verified at a shorter frequency period.
	10.7.1 9.1.4	All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications. (ISO 27002) Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. (ISO 27002)	**Issue:** There are 2 media chambers in the data center for keeping the media. It was found that the humidity range for both the 2 chambers are different The top chamber shows humidity above the red zone (>55%) whereas the bottom chamber is in the green zone (<55%). **Recommendation:** A baseline for the humidity should be documented and checked regularly.	The baseline for the humidity has been identified at 50% and the media chamber humidity checking has been incorporated into the Checklist.

IDA SGCA	ISO 27002:2005	Security Guidelines	Findings & Recommendations	Management Response
2.5.2		Comprehensive CA system review, in the event of a hardware configuration change, software (operating system or layered product) update, network change (hardware, network operating system software or configuration), application update (new application or revised existing application) or changes made to the environment (physical or business) in which the CA functions, shall be conducted periodically.	**Issue:** No evidence that a CA system review was conducted. **Recommendation:** Ensure a CA system review be conducted periodically (eg. Cpu & harddisk utilization)	The last CA review was done on 2008 and we initiated a major CA Infrastructure upgrade in 2009 and we are still currently in the midst of migration. A Comprehensive CA System Review will be conducted once the migration completes.
2.5.4		Network and system security audits shall be performed periodically using automated audit tools to help identify new security vulnerabilities.	**Issue:** There is no evidence that system security audit was perform. **Recommendation:** Ensure that system audit is conducted periodically.	We check our firewall log and IPS log daily as well as the system audit log, system resource and bandwidth utilisation. Penetration and vulnerability test were conducted periodically using Nessus as well.