PKI Audit Methodology
A white paper describing practical methods used to perform PKI compliance audits intended for maximum reliance and affordability

Scott S. Perry CPA, CISA
Solution Leader, IT Risk & Control Services
Slalom Consulting

©2009 Slalom Consulting. All rights reserved.
Introduction

In October 2005, we were approached by a major aerospace company to act as their Compliance Auditor in their effort to become cross-certified with CertiPath LLC, thus gaining acceptance in self-issued credentials in the CertiPath and Federal Bridge Public Key Infrastructures.

Our challenges in adopting an acceptable audit methodology were many:

- No other commercial company had been cross-certified with CertiPath which would have created a precedent to evaluate.
- There is limited current guidance on the audit of public key infrastructures. Much of the groundbreaking standards-setting activities created in the period 1995-to 2001 have not been updated.
- We are not a CPA firm and not licensed to issue a WebTrust certificate for Certification Authorities.

It also created an opportunity for us to establish a new approach to serving all constituents in the process. At Slalom, we view the auditor role in PKI compliance projects as a key one in a company’s pursuit of trustworthy credentials. We see the auditor role as sounding board, arbiter, advisor and empathetic listener - many of these traits at the same time - while maintaining the independence clients and relying parties expect.

Basis for the Methodology

While we had challenges, there were precedents available:

- The Federal Bridge Certification Authority had created a Common Policy Framework for use by participating PKI bridges and Certification Authorities.
- Booz, Allen, Hamilton had created a specification document which provided a template for determining the compliance of a Certification Practice Statement (CPS) with the Common Policy Framework.
- The core of work required is no different than any IT attestation engagement; a party makes assertions requiring reliance by a relying party and accepts an attester’s independent audit activity to generate that assurance.
- Our Company has individuals with a wealth of experience in performing and advising on IT attestation engagements such as SAS 70 and Sarbanes-Oxley compliance efforts.
- CertiPath had a clear desire to provide guidance as soon as practical. On February 16, 2006, CertiPath issued guidelines for the audit of Pre-operational infrastructures. CertiPath did not require a WebTrust certification.

The basis we used in our compliance efforts have been taken from generally accepted IT audit practices and other accepted attestation engagements. In our work, we are given an already approved Certificate Policy (CP). This approval has been made by the relying party or PKI Bridge that requires conformity of any cross-certified or subordinate CA into its PKI. Therefore, this CP serves as the anchor to our work; we
are not asked to provide attestation on the client’s conformity to its bridge or primary CA. It has already been done.

We were asked for attestation and have methodologies in three areas:

1. The level of conformity the client’s Certification Practice Statement has with its Certificate Policy (Called the CP/CPS Compliance Audit).

2. The level of conformity the client’s practices and operational activities have with its Certification Practice Statement prior to full-operation (Called the Pre-Operational Audit).

3. The level of conformity the client’s practices and operational activities have with its Certification Practice Statement after full-operation for a predetermined period of time. CertiPath has asked for attestation for the first six months and yearly thereafter. (Officially called the Operational Audit).

For the three audit projects, we have the following approaches and methodologies:

**CP/CPS Compliance Analysis Methodology**

The essence of the Compliance Analysis is a desk-based design review. The client’s Certificate Policy is delivered as a set of standards that must be achieved similar to a set of control objectives used in a SAS70, SysTrust or Web Trust engagement. The client’s Certification Practice Statement is then reviewed to determine whether the design of activities therein would achieve the associated Policy sections. There is no assurance made at this point on the whether the client’s practices and operational activities conform to its Certification Practice Statement; that is attested to separately.

The CP/CPS Compliance Analysis project is performed in the following three steps:

1. Orientation and Baselining
2. Line-By-Line Analysis
3. Reporting

**Orientation and Baselining**

The first step of the CP/CPS compliance analysis is to thoroughly read the documents to understand the requirements of the CP and CPS. The auditor reviews the documents to ensure the wording contains language that is auditable. Auditable language clearly defines the intent of the client in details that allow evidence to clearly prove that the activities are taking place with reasonable certainty. Auditable language also is conveyed in assertions which are defined as “something declared or stated positively”.

As a result of this initial review process, the auditor provides questions and feedback on the auditability of the documents. At that point, the client must answer the auditor’s questions and should incorporate its feedback into the document which will be used in the next step.
**Line-By-Line Analysis**

After the auditor has a solid understanding of the client’s documents and they are in a format that is auditable, the auditor performs a line-by-line analysis of each section of the client’s CPS to determine how it compares to the CP and whether the design of CPS items will achieve the CP section requirement. Each section is then assessed into one of the following four categories:

1. **Acceptable:** The CPS implements the functionality specified for this CP requirement.

2. **Not Comparable:** The CPS contains dissimilar policy contents, which provides a lower level of assurance/security than the CP requirement.

3. **Missing:** The CPS does not contain procedures that can be compared to the CP requirement in any way.

4. **Not Applicable:** The requirement contained within the CP is not transferable or applied with the CPS.

**Reporting**

The deliverables of the Compliance Audit is an Executive Summary, Cover Letter and Detailed Report. The Detailed Report shows the method used, the versions of the documents, and the representative evidence used to compare the CP and CPS sections. The Detailed Report also contains the assessments of each CP/CPS section. The Cover Letter provides a summary of the method used and the versions of the documents. The Executive Summary contains only the assessments of each CP/CPS sections.
Operational Audit Methodology

**Operational Audit Methodology**

The basis of the pre-operational audit is that the client uses its Certification Practice Statement as its set of assertions they represent to be taking place. They require the compliance auditor to do its due diligence to determine the level of conformity with its CPS.

The compliance auditor divides the CPS into assertions bundled into sections and audited in waves of effort using generally accepted audit techniques until conclusions are reached.

The Operational Compliance Audit project is performed in the following three steps:

1. **Planning**
2. **Fieldwork**
3. **Reporting**

**Planning**

Upon receiving a copy of the CP and CPS, the audit team begins developing an Audit Plan and detailed Test Plans. The Audit Plan contains an initial schedule and organization of test plans into “waves” of effort. Waves are a logical grouping of similar audit activities that can be combined to create greater project throughput. The wave concept also reduces the number of site visits and impact on client team-members. Each wave is approximately one week effort for the audit team.

The audit team works with client management to adjust its audit procedures to balance schedule and impact on team-member work. The resulting Audit Plan sets expectations for schedules and time commitment by client team-members.

The Audit Plan also includes a brief descriptions of acceptable evidence needed to conclude on a section of the CPS.
Fieldwork
As the audit team begins a new wave of audit activities, it communicates in advance all the evidence requirements it needs to conclude on the affected CPS sections. During the audit, the audit team collects this evidence to determine the compliance of the client’s practices and procedures with a standard—the organization’s Certification Practice Statement (CPS). The evidence will be tested using the following four standard audit techniques:

1. **Observation:** a personal visitation and visual review of the current state to determine whether expected conditions are met. This technique is used to determine current settings, physical security and processes in operation.

2. **Examination of Documents:** documents and other printed evidence are inspected for the existence of expected attributes. This technique is used to validate the existence of documents and other documented evidence stated in the CPS.

3. **Reperformance:** the performance of activities by the compliance auditor according to stated process and procedures to validate whether they can be reasonably followed without artificial assistance. This may be used to follow CPS procedures or access CA related systems.

4. **Corroborative Inquiry:** in some cases, interviews of client team-members may be necessary to assess compliance with the activities defined in the CPS. The corroborative inquiry technique will be used in cases where other evidence is not available or possible. *(Note: Inquiry evidence provides the least amount of persuasiveness for validation).*

Reporting
For each section of the CPS, the auditor develops a conclusion based on the evidence available. The following four conclusion categories are reported:

1. **In Compliance:** The PKI was in compliance with the CA’s CPS section assertions.

2. **Partial Compliance:** The PKI was in compliance with some of the CA’s CPS section assertions.

3. **Not In Compliance:** The PKI was not in compliance with the CA’s CPS section assertions.

4. **Not Applicable:** The assertions contained in the CA’s CPS section were not auditable or did not contain assertions to audit.

As previously stated, the conclusions for each assertion are based on collected evidence. Each conclusion is documented by the Auditor and the evidence defined as of the date of the Cover Letter. The Lead Auditor on the project performs a quality review of test plans and results to ensure consistency and accuracy of conclusions. The Lead Auditor then issues an Executive Summary Report and Cover Letter. All workpapers are delivered to the client who retains custody of them.
Operational Audit Methodology

CertiPath requires operational audits after the first six months of operation and then every year thereafter. Audit procedures for the operational audit are the same as the pre-operational audit with a couple of exceptions.

The conclusion and the assurance provided by the auditor are for a period of time (e.g. six months, one year) as opposed to one point of time. Therefore, the audit team must extend its procedures to satisfy themselves over the coverage period. This includes two major methodology differences than the pre-operational audit:

1. The auditor should audit CPS assertions multiple times during the coverage period to satisfy themselves that the procedures were being complied with consistently during that time. If procedures are not being followed consistently, this would be considered a reportable exception and highlighted as part of audit findings under *Partial Compliance*.

2. While pre-operational audit activities have limited sample sizes, operational audits over six or twelve months may include hundreds or thousands of transactions. The auditor therefore extends the audit plan to ensure sample sizes and site visits are appropriately representative to conclude on the transaction population.
Bibliography


PKI Assessment Guidelines, Public Draft for Comment June 18, 2001, Information Security Committee, Electronic Commerce Division, Section of Science, Technology & Law, American Bar Association

Certipath Commercial PKI Bridge, Pre-Operational Audit Guidelines, February 16, 2006

AICPA/CICA WebTrust Program for Certification Authorities, August 25, 2000 Version 1.0, American Institute of Certified Public Accountants, Inc., and Canadian Institute of Chartered Accountants

Suitable Trust Services Criteria and Illustrations, American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, 2003


Information Systems Control Journal, Volume 5, 2002, Auditing and Certification of a Public Key Infrastructure By Ronald Koorn, MSc., CISA, RE, Peter van Walsem, MSc., and Mark Lundin, MSc., CISA, CPA

FICC Audit Standards for PKI Shared Service Provider Entities: An Analysis of Requirements and Alternatives, Federal Identity Credentialing Committee and the Shared Service Provider Subcommittee, January 16th, 2004