PKI Auditing Guideline

Office of the Controller of Certifying Authorities

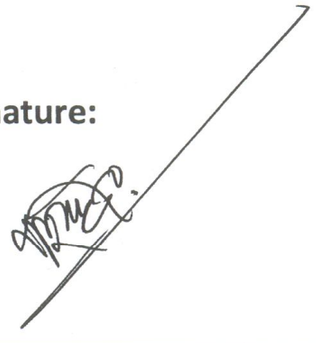
Ministry of Information & Communication Technology

Government of the Peoples Republic of Bangladesh

Document Reference

Document Title	PKI Auditing Guideline
Document Type	Public
First Publishing Date	December 2010
Version	1.01
Last Update	January 2012
Pages	18
Status	Approved

Signature:



(Md. Zahangir Alam, ndc)
Controller of Certifying Authorities

Table of Contents

Introduction

According to the IT (CA) Rules 2010, any Certificate Authorities (CAs) licensee needs to be audited before commencing its operation and also yearly two auditing would be required for its continuation of operation. The main purpose of the auditing is to check the compliance of the CA against the set forth rules, procedures and the practices which governed its operations. The CA should abide by the terms and conditions mentioned in the license condition document. As per the terms and conditions; a CA will be audited for his infrastructure, security procedures etc.

Purpose of auditing

The compliance auditor will communicate results of all compliance audits to the Policy Authority (PA) through a Compliance Audit Report. The report will contain a summary table of topics covered, areas in which the CA was found to be non-compliant, and a brief description of the problem(s) for each area of non-compliance. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the CA passed and the topics in which the CA failed. Notification of compliance audit failure, the topics of failure, and reason(s) for failure will be provided immediately, upon the conclusion of the compliance audit, in a written form to the PA.

Scope of the Auditing

Users should use X.509 certificates for authentication and authorization. Those certificates are typically issued by Certificate Authorities (CAs) operated by real institutions those compose a virtual organization. In order to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures, those Certificate Authorities should be audited. Processes of auditing include an independent examination of documentation, records, activities to access the adequacy of system controls, interview to the staffs in charge of administration and operation of the Certificate Authority, and inspections of evidences and physical devices, etc.

2.1 Frequency and Duration of Auditing: The operation of any licensee CAs could be started after the first auditing (Rules-21(C)). After that, all operational CAs would be audited as per Rules 32(2) and the report should be completed in compliance with Rules 32(3).

2.2 Out of Scope: The sole purpose of this auditing is technical and procedural. And

hence, any financial auditing of CAs is out of scope for this auditing.

Appointment of Auditor

The controller would create a panel of auditor or audit firm according to Rules 33(2). However, the relationship between CA and Auditor would be governed by Rules 33(1) and 33(3).

Audit Checklist

The proposed criteria consist of the following three principles (not limited to)

- **Principle 1: CA Business Practices Disclosure**
  - The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices

- **Principle 2: Service Integrity**
  - The certification authority maintains effective controls to provide reasonable assurance that:
    1. Subscriber information was properly authenticated (for the registration activities performed by CA) and
    2. The integrity of keys and certificates it manages is established and protected throughout their life cycles.

- **Principle 3: CA Environmental Controls**
  - The certification authority maintains effective controls to provide reasonable assurance that: (1) Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure; (2) The continuity of key and certificate life cycle management operations is maintained; and (3) CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.

Procedures of auditing

A list of marks for auditing

Auditors prepare a list of marks for auditing, which is a table of the audit checklist,

evidences, procedures and results of the examination, and scores of the items in the audit checklist. Each item in the audit checklist should be scored according to the results of the examination. For example, each item can be scored from A to D, and X as below.

- A: Good.
- B: Recommendation (minor change)
- C: Recommendation (major change)
- D: Advice (must change)
- X: Could not evaluate (N/A)

The CA cannot start/continue its operation with score C, D and X. For score B a CA can start/continue its operation by monitoring a date approved by the controller and by which he must make necessary changes as per the audit recommendations.

Materials used for auditing

Auditing consists of a pre-examination, a main examination, and a post examination. In the pre-examination, all possible documents available for the auditors are examined. The followings are examples of those documents.

- CP of each certificate class.
- CPS
- Manuals for subscribers (e.g. enrollment manual)
- Operational manuals (for CA operators)
- CA Repository (e.g. Web site)
- CA Certificate
- Certificate Revocation List (CRL)
- End entity certificates
- Hardware security module (**HSM**) manual (or appropriate web site)
- Any other document described as "published on the repository" in the CP/CPS such as Quarterly Internal Audited Documents
- Any other document available for the auditors

Some of these documents must be available on the repository and the auditors could request the CA to provide the other documents.

In the main examination, the auditors visit the CA and interview the staffs in charge of administration and operation of the CA, and inspect evidences and physical devices, etc.

The followings are examples of subjects of the inspection.

- CA room
- HSM
- A place (e.g. a safe box) for keeping a backup media of the CA private key
- A place (e.g. a safe box) for keeping media storage of archived logs and other documents
- CA operating machine and devices.
- End entity certificates (if not available for the pre-examination)
- Logs of the CA/RA servers
- Logs of the CA repository (e.g. Web server)
- Records of operation of the CA private key (including accesses to the HSM)
- Access log to the CA room
- Any other documents (e.g. daily report of the CA operators)

Pre-Examination

In the pre-examination, the auditors evaluate each item in the audit checklist by examining appropriate materials available for the auditors for the pre-examination. Some of the items could be scored according to the results of the pre-examination, but some of the items may need an interview to the CA operators and inspections to be scored. Necessary evidences for the evaluation depend on available materials and their usefulness for the pre-examination. If the auditors could not score an item, the auditors should describe necessary examinations, interviews, and inspections in the list of marks for auditing, which will be carried out during the main examination.

Main Examination

In the main examination, the auditors visit the CA, interview to the CA staffs, and inspect documents **(e.g. archived logs) and equipments (e.g. CA server, HSM, backup media, etc) according to the results** of the pre-examination. The auditors should score the items which could not be scored in the pre-examination.

Post-Examination

In the post-examination, the auditors draft an auditing report according to the results of the pre-examination and the main examination. The audit report should include the

followings:

- Date of auditing
- Terms of subjects of auditing
- Names of the auditors
- Names of the participants
- Results of the auditing
  - Scores of the items in the audit checklist
  - Comments for Scores B, C, and D.

The auditing report should be drafted and sent to the CA within four weeks after the auditing. The CA is expected to send a report on the plans for improving the CA operation to the auditors within four weeks of receiving audit report. A copy of all these documentations must be reported to CCA for its satisfaction.

Responsibilities of an Auditor and Auditee

The responsibilities of an Auditor (empanelled auditor) and Auditee (CA) have been extracted from **RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** and in accordance with ICT Act 2006 and IT (CA) Rules 2010. Licensed CAs and empanelled auditors must comply with the audit criteria from their respective role.

A. Publication, Repository and Records Archival

The licensed CA and the empanelled auditor must address the following issues (not limited to) related to certificate repository and publishing necessary information from their respective role:

- Publication of CPS in web
- Object Identifier (OID) for CPS
- CPS Administration
- Publication of Certificate information in web
- Repository management and accessibility method
- Access control for Repository
- Information archiving procedure with time-stamping and retention period
- Archive protection procedure
- Archive backup procedure

B. Identification and Authentication

Regarding identification and authentication of RA, subscriber, relying parties and other entities interoperating with PKI, the CA and Auditor must address the following measures:

- Naming as per the **Certifying Authority Interoperability Guideline**
- Identity Validation procedure of RAs, Subscribers and other parties for each type of certificates and PKI services.
- Identification and authentication procedure for re-key and revocation request

C. Non-technical security controls

Non technical security controls are so critical since lack of security may cause compromise of CA operation. Non technical security controls are physical, procedural and personnel controls performs by CA. The auditor must check how a CA is conforming the non technical security controls in its CA operation. Following matters must be considered by both CA and Auditor:

- CA must have a security policy for non technical security;
- Physical security controls (such as site location, construction of highly secured zone, strong room, physical access control, power condition, air-conditioning and heat protection, fire prevention and protection, water exposures, waste disposal, dust protection etc.)
- Procedural controls
    - Define trusted role for administration of CA operations (such key generation, subject authentication, certificate issuance, certificate revocation, auditing, archiving etc.);
    - Distribution of tasks (n out of m rule) should be stated for each role;
    - Separation of role.
- Personnel Security Controls
    - Trusted personnel hiring procedure;
    - Trusted personnel background check and clearance;
    - CCA approval for trusted personnel;
    - Controls on personnel.
- Logging procedure for every CA operation
    - events record procedure;
    - Backup and archiving procedure of audit logs;
    - Duration of keeping audit and event logs;
    - Protection of logs;
    - Trusted personnel hiring procedure;
    - Trusted personnel background check and clearance;

- Vulnerability assessment;
- Strong room access registers with reasons.

- Identification of probable compromises, incidents and disasters;
- Compromise, incidents and disaster recovery procedure;
- RA termination and RA records archiving procedure.

D. Technical security controls

Technical security controls are the security measures taken by the CA to perform securely the function of key generation, cryptographic key protection, protection of activation data, authentication of the requester, certificate issuance, revocation, archiving etc.

The auditor must prepare audit checklist to inspect how a CA conforms their technical security controls, such as:

- CA must have a security policy for technical security;
- Assets must be classified;
- CA, RAs or subscribers key pair generation and installation procedure;
- FIPS 140-2 level 3 capable hardware to generate key pair;
- Security measures taken if key pair delivered over the internet to the subscriber/RAs;
- Secure session while receiving and issuing certificate request along with public key of an entity;
- Key sizes (CA, RAs, Subscribers) as per **Certifying Authority Interoperability Guideline**;
- CA private key control (n out of m rule);
- Private key storing procedure (in hardware or software module);
- Public key of CA must be distributed in manner so that the integrity and authenticity of the key is ensured;
- Key backup and archiving procedure;
- Key escrow procedure with reasonable assurance;
- Operational period of the certificate as per the Certificate validity notification issued by CCA;
- Computer security controls;
- Network security controls;
- Time-stamping (Sync with National Time Server).

E. Certificate Lifecycle Management

Certificate lifecycle management includes CA, RAs, Subscribers and other entities. CA and auditor must take care of the following issues, such as:

- Certificate Application/Enrollment process from RAs/Subscribers/other parties;
- Procedure for validation of certificate request, RA signature;
- CA to RA communication for CSR and Certificate;
- Procedure for certificate issuance to the end entities through web or directly;
- Confirmation of certificate acceptance or rejection by the end entities;
- Publication of certificate in a directory/repository;
- Certificates, CRLs and OCSP profile must comply with the **Certifying Authority Interoperability Guideline**;
- Define RA, Subscriber, and Relying party responsibility relating to the certificate;
- Certificate renewal and re-key procedure;
- Certificate revocation and suspension procedure;
- OCSP for knowing certificate status;
- Procedure for end of subscription of certificate.

F. Key Life Cycle Management

A CA must securely handle his own key pair and the key pair of RA and subscriber (if the CA generates and manages subscriber's key). The auditor must inspect how a CA manages a key throughout of its lifecycle.

For CAs own Key:

- Key generation algorithm as per **Certifying Authority Interoperability Guideline**
- The key size must be 2048 bit
- cryptographic module to generate keys (ISO 15782-1/FIPS 140-1/ANSI X9.66 level standard)
- Purpose and usage restriction of the key
- key validity as per the Notification issued by Controller;
- CA private key must be maintained using multi person control (m out of n rule)
- CA private signature key is escrowed with reasonable assurance
- CA private signing key is backed up and public signature keys are archived

Subscriber Key:

- Key generation algorithm as per **Certifying Authority Interoperability Guideline**
- The key size must be 1024 bit
- cryptographic module to generate keys (ISO 15782-1/FIPS 140-1/ANSI X9.66 level standard)

- Purpose and usage restriction of the key
- Key validity as per the Notification issued by Controller;
- Subscriber's private key must be provided securely to the subscriber
- Subscriber's decryption private key is backed up and archived
- Conditions for destroying a subscriber's private key
- Subscriber private decryption keys are escrowed by the CA.
- Routine rekey with description of the identification and authentication and rekey request verification procedures;
- Rekey after revocation or expiration, including a description of the identification and authentication and rekey request verification procedures;
- Certificate distribution with description of the CA's established mechanism for making available to relying parties the certificates and Certificate Revocation Lists that it issues.

G. Compliance with ICT Act 2006 and IT(CA) Rules 2010

This part is very important for both CA and empanelled auditor. The CA must comply with ICT Act 2006 and IT (CA) Rules 2010 while doing CA operation. Significant areas of the Act and Rules for auditing CA that must be considered are:

- Section 16 and 17 of the ICT Act 2006 for secure electronic record and signature;
- Section 31 of the ICT Act 2006 related to CA operation of Certifying Authority;
- Section 35 of the ICT Act 2006 for publication of information by CA;
- A CA must follow the certificate issuance condition mentioned in Section 36 of the ICT Act 2006 and Rule 24, 25, 26 of IT (CA) Rules 2010;
- Assurance by a CA for certificate as per Section 37 of the ICT Act 2006;
- CA must comply with certificate revocation and suspension procedure mentioned in Section 38, 39 and 40 of the ICT Act 2006;
- CA must aware their subscriber/end users about their responsibility mentioned in Section 41, 42, 43 and 44 of the ICT Act 2006;
- Actions or procedure taken by a CA to protect issuance of fake certificate (Section 64 and 65 of the ICT Act 2006);
- Procedure for digital signature creation as per Rule 4 of IT (CA) Rules 2010;
- Procedure for signature validation as per Rule 5 of IT (CA) Rules 2010;
- Standard to be followed by a CA is mentioned in Rule 7, 8 of IT (CA) Rules 2010;
- Cross-certification issue as per Rule 14 of IT (CA) Rules 2010;
- CA Security related to dos as per Rule 20 of IT (CA) Rules 2010;
- Rule 21 of IT (CA) Rules 2010, before commencing CA operation;

- CA operation termination procedure as per Rule 22 of IT (CA) Rules 2010;
- Certificate repository as per Rule 28 of IT (CA) Rules 2010;
- CA and auditor must comply with Rule 32, 33 of IT (CA) Rules 2010;
- Privacy of information as per Rule 34 of IT (CA) Rules 2010.

H. CA System and Services administration

The CA system is very important part in CA operation. CA system must be dedicated machine for each of its services and operations and must ensure highest level of security and quality of service. It includes:

- Dedicated system for CA, must be isolated logically and physically from any other services;
- Physical security;
- Software Security, OS Security;
- Algorithm compliance as per **Certifying Authority Interoperability Guideline**;
- Physical and logical security of HSM;
- FIPS 140-2 validated Cryptographic Module;
- Cryptographic module must be accessible to limited trusted personnel;
- Trusted software development methodology;
- Integrity of software, hardware, firmware;
- Product maintenance procedure;
- Logical security of Database;
- Must use sufficient physical and logical security to protect the CA System from outside or inside attack;
- RA service administration procedure;
- CA must ensure proper assurance to manage subscribers key and certificate;

I. Operational Audit

As per the Sub-Rule 32(2) and to comply with Rule 32 and 33 of IT (CA) Rules 2010, A CA must have periodical internal operational audit. As mentioned in Sub-Rule 32(2), A CA must have audit twice in a year for CA operation, non technical and technical security controls and quarterly in a year for its repository. CA must prepare and submit its procedure of operational audit to the Controller. Controller or his designated officer can verify the submitted internal audit report.

Conclusion

This guideline could be changed time to time by the Controller, as and when necessary.

Appendix A: Sample Report Illustration

Unqualified Opinion

Report of Independent PractitionerTo the Management of ABC Certification Authority, Inc.:

We have examined the assertion [hot link to management assertion] by the management of ABC Certification Authority, Inc. (ABC-CA) [hot link to management's assertion] that during the period Xxxx xx, 200x through Yyyy yy, 200x, for its Certification Authority (CA) operations at LOCATION, ABC-CA, ABC-CA has:

- Disclosed its Digital Certificate life cycle management practices and procedures, including its commitment to provide Digital Certificates in conformity with the CA Guidelines, and provided such services in accordance with its disclosed practices, and
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by ABC-CA) and verified, and
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles, based on Certification Authorities - Audit Criteria [hot link to Controller of Certification Authorities - Validation Criteria].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the CCA, and accordingly, included (1) obtaining an understanding of ABC-CA's certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of certificates; (2) selectively testing transactions executed in accordance with disclosed certificate life cycle management practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, ABC-CA management's assertion, as referred to above, is fairly stated, in all material respects, based on the Controller of Certification Authorities Validation Audit Criteria. Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing

requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations. This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the Controller of Certification Authorities - Validation Criteria, or the suitability of any of ABC-CA's services for any customer's intended purpose.

[Name of Audit firm]

[City, State]

[Date]

Appendix-B: Audit Checklist

This Certifying Authority (CA) Audit Checklist is prepared by the Office of the CCA to carry out the first audit of the Certifying Authority by the empanelled auditor. The auditee (CA) and the auditors must follow this checklist along with this Guideline issued by the Office of the CCA.

CA Audit Checklist

Sl.	Audit Criteria	Evaluation Method		Remarks
		Yes/No	Level/Score	
1.	Is the CPS published in the website of the CA?			
2.	Does the CPS have valid Object Identifier (OID)?			
3.	Is CA Certificate information published in their web?			
4.	Is repository management and accessibility method available?			
5.	Does CA have Identity Validation procedure of RAs, Subscribers and other parties?			
6.	Evaluate Physical security controls (such as site location, construction of highly secured zone, strong room, physical access control, power condition, air-conditioning and heat protection, fire prevention and protection, water exposures, waste disposal, dust protection etc.)?			
7.	Is the task distributed (n out of m rule) and defined for each role for administration of CA operations?			
8.	Is there any trusted personnel hiring procedure?			
9.	How a CA does background check of trusted personnel?			
10.	How CA keep controls on its personnel?			
11.	Is there any events record procedure?			
12.	Does CA take backup of audit logs?			

Sl.	Audit Criteria	Evaluation Method		Remarks
		Yes/No	Level/Score	
13.	Does CA maintain Strong room access logs?			
14.	Is RA termination and RA records archiving procedure defined?			
15.	Check whether the hardware to generate key pair of CA/RAs/Subscribers is FIPS 140-2 level 3 capable?			
16.	Does CA take proper security measures for key pair to be delivered over the internet to the subscriber/RAs?			
17.	Is there any secure session while receiving and issuing certificate request along with public key of an entity?			
18.	Key sizes (CA, RAs, Subscribers) as per **Certifying Authority Interoperability Guideline?**			
19.	Does CA control its private key by following **n out of m rule**?			
20.	Does CA store Private key in FIPS 140-2 level 3 capable hardware?			
21.	How CA ensures the integrity and authenticity of its Public key in while it's distributed?			
22.	Does CA maintain Key backup and archiving procedure properly?			
23.	Does CA maintain Key escrow procedure with reasonable assurance?			
24.	Does CA follow Certificate validity notification issued by CCA for certificate validity?			
25.	Is the computer and network security controls sufficient?			
26.	Is Certificate Application/Enrollment process of RAs/Subscribers/other parties as per the CPS?			
27.	Is the CA to RA communication sufficiently secure for CSR and Certificate?			
28.	Does Certificates, CRLs and OCSP profile comply with the **Certifying Authority Interoperability Guideline**?			
29.	Certificate renewal and re-key procedure as per CPS?			
30.	Certificate revocation and suspension procedure as per CPS?			

Sl.	Audit Criteria	Evaluation Method		Remarks
		Yes/No	Level/Score	
31.	Does CA maintain its private key using multi person control (m out of n rule)?			
32.	Does the Subscriber's private key provided securely to the subscriber?			
33.	Subscriber's decryption private key is backed up and archived?			
34.	Are the conditions for destroying a subscriber's private key stated?			
35.	Does CA maintain proper security mechanism to escrow subscriber private decryption keys?			
36.	Does CA maintain any mechanism for certificate and CRL distribution?			
37.	Does CA maintain standards as mentioned in the Certificate Interoperability Guideline?			
38.	Is the CA system isolated logically and physically from any services other than CA?			
39.	Does CA have Software Security, OS Security procedure?			
40.	Algorithm compliance as per **Certifying Authority Interoperability Guideline**?			
41.	Is there any Physical and logical security of HSM?			
42.	Is the software development methodology trusted?			
43.	Evaluate software, hardware, firmware for their Integrity?			
44.	Is there any physical and logical security to protect the CA System from outside or inside attack?			

For this check list Level/Score might be according to the score mentioned in the PKI Auditing guideline. Auditor will state findings or reasons for this type of evaluation in the Remarks column.