# Certification Practice Statement (CPS) Guidelines

Controller of Certifying Authorities, Bangladesh

## Office of the Controller of Certifying Authorities

Ministry of ICT

Government of Bangladesh

# Document Reference

| | |
|---|---|
| Document Title | Certification Practice Statement (CPS) Guidelines |
| Document Type | Public |
| Publishing Date | December 2010 |
| Version | 1.0 |
| Last Update | December 2010 |
| Pages | 15 |
| Status | Approved |

**Signature:**

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

## Table of Contents

## List of Abbreviations/Acronyms

| | |
|---|---|
| CA | Certificate Authority |
| CCA | Controller of Certifying Authority |
| CP | Certificate Policy |
| CPS | Certificate Practice Statement |
| CRL | Certificate Revocation List |
| ICT | Information & Communication Technology |
| IT | Information Technology |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RFC | Request for Comments |

## Executive Summery

The Certificate of Practice Statement (CPS) is the core charter for Certifying Authority (CA). This guideline for CPS shall be in addition to the provision laid down under Information and Communication Technology Act 2006 and subsequent IT (CA) Rules 2010 to operate as a CA.

This CPS guideline is based on *RFC-3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,* November 2003

## 1. INTRODUCTION

The certificate practice statement (CPS) translates certificate policies into operational procedures on the CA level. The certificate policy focuses on a certificate while the CPS focuses on a CA.

A CPS might include the following types of information: a) Positive identification of the CA, including the CA name, server name, and Domain Name System (DNS) address; b) Certificate policies that are implemented by the CA and the certificate types that are issued; c) Policies, procedures, and processes for issuing, renewing, and recovering certificates; d) Cryptographic algorithms, cryptographic service providers (CSPs), and the key length that is used for the CA certificate; e) Physical, network, and procedural security for the CA; f) The certificate lifetime of each certificate that is issued by the CA; g) Policies for revoking certificates, including conditions for certificate revocation, such as employee termination and misuse of security privileges; h) Policies for certificate revocation lists (CRLs), including where to locate CRL distribution points and how often CRLs are published and i) A policy for renewing the CA's certificate before it expires. The CPS should not limited to these items.

This guideline introduces a set of provisions and indicates types of practice for prospective CA. The CPS is the core practice guideline of CA. The technology and operational procedure might be changed time to time and any new procedure has to be incorporated in the CPS. However, any change in the CPS needs to be approved by the Controller of certificate authority and only after such approval the new CPS would be effective. CAs are bound to made the CPS available publicly.

## 2. THE CPS OUTLINE

The CPS should be based on RFC-3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. However, the following provisions had to be incorporated in the CPS. The CPS should conform the ICT Act 2006 and IT (CA) Rules 2010.

### A. INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted. Subcomponents under this component should include but not limited to:

- Overview
- Document name and identification
- PKI participants
- Certificate usage
- Policy administration
- Definitions and acronyms

### B. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This component contains identification of the entity or entities that operate repositories within the PKI, responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, frequency of publication and access control on published information. Subcomponents under this component must include:

- Repositories
- Publication of certification information
- Time or frequency of publication
- Access controls on repositories

### C. IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance and revocation. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. This component also addresses naming practices, including the recognition of trademark rights in certain names. The Subcomponents are:

- Naming
- Initial Identity Validation
- Identification and authentication for re-key requests
- Identification and authentication for revocation request

### D. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate. Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants. Subcomponents are:

- Certificate Application
- Certificate application processing
- Certificate issuance
- Certificate acceptance
- Key pair and certificate usage
- Certificate renewal
- Certificate re-key
- Certificate modification
- Certificate revocation and suspension
- Certificate status services
- End of subscription
- Key escrow and recovery

## E. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject (CAs, RAs, subscribers) authentication, certificate issuance and revocation, archiving, auditing, repositories management, and other participants and CA operations. Subcomponents are as follows:

- Physical controls
- Procedural controls
- Personnel controls
- Audit logging procedures
- Records archival
- Key changeover
- Compromise and disaster recovery
- Sub CA or RA termination

## F. TECHNICAL SECURITY CONTROLS

This component is used to define the technical security measures taken by the issuing CA to protect its cryptographic keys and activation data. This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, subject (CAs, RAs, subscribers) authentication, certificate issuance and revocation, archiving, auditing, repositories management, and other participants and CA operations. Subcomponents are as follows:

- Key pair generation and installation
- Private Key Protection and Cryptographic Module Engineering Controls
- Other aspects of key pair management
- Activation data

- Computer security controls
- Life cycle technical controls
- Network security controls
- Time-stamping

## G. CERTIFICATE, CRL, AND OCSP PROFILES

This component is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used. Subcomponents under this component are:

- Certificate profile
- CRL profile
- OCSP profile

## H. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This component addresses the list of topics covered by the assessment, frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, the identity and/or qualifications of the personnel performing the audit or other assessment, the relationship between the assessor and the entity being assessed, including the degree of independence of the assessor, actions taken as a result of deficiencies found during the assessment; person entitled to see results of an assessment. Subcomponents under this component must include:

- Frequency or circumstances of assessment
- Identity/qualifications of assessor
- Assessor's relationship to assessed entity
- Topics covered by assessment
- Actions taken as a result of deficiency
- Communication of results

## I. OTHER BUSINESS AND LEGAL MATTERS

This component covers general business and legal matters. This component must address the following issues:

- Fees
- Financial responsibility
- Confidentiality of business information
- Privacy of personal information
- Intellectual property rights
- Representations and warranties
- Disclaimers of warranties
- Limitations of liability
- Indemnities
- Term and termination
- Individual notices and communications with participants
- Amendments

- Dispute resolution provisions
- Governing law
- Compliance with applicable law
- Miscellaneous provisions
- Other provisions

## 3. SPECIAL NOTE

Controller of Certifying Authority suggests four classes of certificate to be issued by a CA. In addition to four classes of certificates given below, the Certifying Authority may issue more type of certificates, but these must be explicitly defined (in CPS) including the purpose for each type of certificates and the verification methods underlying the issuance of the certificate. The suggested certificate classes are given below:-

***Class 0 Certificate***: This certificate shall be issued only for demonstration/ test purposes.

***Class 1 Certificate:*** Class 1 certificate shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database such as national id database, passport database etc.

***Class 2 Certificate:*** These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

***Class 3 Certificate:*** This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities with appropriate documents.

## 4. SAMPLE OUTLINE

This is a sample outline for CPS taken from RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework:-

------------------------------------------------------- **Beginning of Document** --------------------------------------------------

1. INTRODUCTION

1.1 Overview

1.2 Document name and identification

1.3 PKI participants

1.3.1 Certification authorities

1.3.2 Registration authorities

1.3.3 Subscribers

1.3.4 Relying parties

1.3.5 Other participants

1.4 Certificate usage

1.4.1. Appropriate certificate uses

1.4.2 Prohibited certificate uses

1.5 Policy administration

1.5.1 Organization administering the document

1.5.2 Contact person

  - 5.3.3 Training requirements
  - 5.3.4 Retraining frequency and requirements
  - 5.3.5 Job rotation frequency and sequence
  - 5.3.6 Sanctions for unauthorized actions
  - 5.3.7 Independent contractor requirements
  - 5.3.8 Documentation supplied to personnel
- 5.4 Audit logging procedures
  - 5.4.1 Types of events recorded
  - 5.4.2 Frequency of processing log
  - 5.4.3 Retention period for audit log
  - 5.4.4 Protection of audit log
  - 5.4.5 Audit log backup procedures
  - 5.4.6 Audit collection system (internal vs. external)
  - 5.4.7 Notification to event-causing subject
  - 5.4.8 Vulnerability assessments
- 5.5 Records archival
  - 5.5.1 Types of records archived
  - 5.5.2 Retention period for archive
  - 5.5.3 Protection of archive
  - 5.5.4 Archive backup procedures
  - 5.5.5 Requirements for time-stamping of records
  - 5.5.6 Archive collection system (internal or external)
  - 5.5.7 Procedures to obtain and verify archive information
- 5.6 Key changeover
- 5.7 Compromise and disaster recovery
  - 5.7.1 Incident and compromise handling procedures
  - 5.7.2 Computing resources, software, and/or data are corrupted
  - 5.7.3 Entity private key compromise procedures
  - 5.7.4 Business continuity capabilities after a disaster
- 5.8 CA or RA termination

**6. TECHNICAL SECURITY CONTROLS**

- 6.1 Key pair generation and installation
  - 6.1.1 Key pair generation
  - 6.1.2 Private key delivery to subscriber
  - 6.1.3 Public key delivery to certificate issuer
  - 6.1.4 CA public key delivery to relying parties
  - 6.1.5 Key sizes
  - 6.1.6 Public key parameters generation and quality checking
  - 6.1.7 Key usage purposes (as per X.509 v3 key usage field)
- 6.2 Private Key Protection and Cryptographic Module Engineering Controls
  - 6.2.1 Cryptographic module standards and controls
  - 6.2.2 Private key (n out of m) multi-person control
  - 6.2.3 Private key escrow
  - 6.2.4 Private key backup
  - 6.2.5 Private key archival
  - 6.2.6 Private key transfer into or from a cryptographic module
  - 6.2.7 Private key storage on cryptographic module
  - 6.2.8 Method of activating private key
  - 6.2.9 Method of deactivating private key
  - 6.2.10 Method of destroying private key
  - 6.2.11 Cryptographic Module Rating
- 6.3 Other aspects of key pair management
  - 6.3.1 Public key archival
  - 6.3.2 Certificate operational periods and key pair usage periods
- 6.4 Activation data
  - 6.4.1 Activation data generation and installation

------------------------------------------------------------- **End of Document** --------------------------------------------------------