CERTIFYING AUTHORITES PERSONNEL (QUALIFICATION ANDEXPERIENCE) GUIDELINES

Version: 1.0

30 June 2024

Office of the Controller of Certifying Authorities
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology

Document Control

Document Name	CERTIFYING AUTHORITES PERSONNEL (QUALIFICATION AND EXPERIENCE) GUIDELINES
Version	1.0
Status	Approved
Last update	30 June 2024
Document Type	Public
Document Owner	Office of the Controller of Certifying Authorities, Bangladesh.

Contents

1. Introduction

1.1 Background

The Office of the Controller of Certifying Authorities issues Licences to Certifying Authorities (CA) under section 22 of the Information and Communication Technology Act, 2006 after duly processing their applications as provided for under the Act. Licensed Certifying Authorities (CAs) are required to recruit its personnel for its operation in a proper manner. The Controller shall determine the required qualifications and experience of the employees of the Certifying Authorities as per the section 19(c) of the Information and Communication Technology Act, 2006.

1.2 Purpose

Objective of this guidelines is to ensure the reliability and trustworthiness of the operation of the Certifying Authorities by determining the required qualifications and experience of their employees as well as to ensure, protect, and clarify the rights and responsibilities of both the employer and employees of the Certifying Authorities.

1.3 Scope

Subject to such conditions and limitations as specified in the Information and Communication Technology Act, 2006, or Rules made thereunder, the provisions of this guidelines shall extend to thepersonnel of the Certifying Authorities.

2. Definitions

In these Guidelines unless there is anything repugnant in the subject or context: -

"Act" means Information and Communication Technology Act, 2006 (Act No. 39 of 2006).

"Certifying Authority" or **"CA"** means Certificate Issuing Authority as defined in Information and Communication Technology Act, 2006 (Act No. 39 of 2006)."

"Electronic Signature Certificate" or **"Digital Signature Certificate"** means any electronic signature certificate as defined in Information and Communication Technology Act, 2006 (Act No. 39 of 2006).

"Independent Contractor" means any person other than the employees carrying out the duties of thetrusted roles in the operation of Certifying Authorities.

"Personnel" means any person employed or engaged in the operation of Certifying Authorities.

"Registration Authority" or **"RA"** means an entity that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications

for renewal or re-keying certificates on behalf of a Certifying Authority.

"Trusted Person" means any person who has: -

a) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or Rules in respect of a Certifying Authority, or
b) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration ofa Certifying Authority's computing facilities.

3 Appointment of CA Personnel

3.1 Method of Appointment

Subject to the provisions set out in this guideline the appointment to any personnel, performing dutiesin the operation of any certifying authority, shall be made in writing by an approving authority in the manner described below:

a) by direct recruitment;
b) by deputation;
c) Independent Contractor.

The Certifying Authority must ensure that no person shall be appointed to the operation of any Certifying Authority unless he/she-

a) possess the qualifications, experience, and clearance requirements; and
b) complete background check procedures.

The list of the appointed personnel, performing duties in the operation of any certifying authority, shall be sent to the Controller for approval.

3.2 Appointing Authority

The Certifying Authority or any other entity responsible for the appointment of personnel on behalf of the Certifying Authority shall be deemed to be the Appointing Authority unless otherwise providedin any other laws, rules, regulations, policy, guideline, or statutes.

3.2. General Requirements

All personnel of the Certifying Authority must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation. Personnel appointed to trusted roles (CA trusted roles) shall:

a) Be trustworthy;
b) Have successfully completed an appropriate training program;
c) Have demonstrated the ability to perform their duties;
d) Have no other duties that would interfere or conflict with their duties for the trustedrole;
e) Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
f) Have not been denied a security clearance, or had a security clearance revoked forcause; and
g) Have not been convicted of a felony offense.

3.3. Background checks and clearance procedures

3.4.1. Prior to commencement of employment, the Human Resource Department of the Certifying Authority must conduct the background checks. Trusted Roles must receive a favorable adjudication after undergoing a background investigation in the following areas:

a) Identification card
b) Confirmation letter of previous employment
c) Certificate of the highest education
d) Place of residence;
e) Criminal records (Law Enforcement);
f) Misrepresentations by the candidate;
g) Professional certificate (if any)
h) Any clearances as deemed appropriate;
i) Background Check (Recheck at least every three years);
j) References.

3.4.2. The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with Bangladeshi laws, or equivalent.

3.4.3. The Certifying Authority may also exercise other measurements for background checkwhen necessary. If the provided information is found to be false, or if the education/professional background is found unmatched, or if the person has

certain criminal convictions, that person shall not be eligible to work with the Certifying Authorities.

3.4.4. The Certifying Authority shall maintain confidentiality and privacy of personal information of any personnel in a reasonable manner during background check. Background check procedures shall be described in the Certification Practice Statement of the Certifying Authorities.

4 Training of CA Personnel

4.1.Training requirements and training procedures

The Certifying Authority must provide its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to CAoperations with competency and satisfaction. The training programs include the following asrelevant:

a) All PKI duties they are expected to perform;
b) Basic cryptography and Public Key Infrastructure (PKI) concepts;
c) Information Security Awareness;
d) Use and operation of all PKI hardware and software versions deployed to CAoperations;
e) Security Risk Management;
f) Disaster recovery and business continuity procedures;
g) Security Principles and Mechanisms;
h) Common threats to the validation process, including phishing and othersocial engineering tactics;
i) Applicable Industry and Government guidelines.

Certifying Authority shall ensure personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. All Validation Specialists shall pass an examination provided by the CA on the information verification requirements.

4.2. Retraining period and retraining procedures

The CA must provide its officers with appropriate training at least once a year on the relatedtopics and information security awareness. Whenever there is any change in the Issuer CA's,ESP, or RA's operations appropriate training is provided to the individuals acting in trusted roles so that they are aware of the changes.

Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

Refresher training must be conducted as and when required. Records of all trainings shall bemaintained and reviewed periodically. Periodic training updates will be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5 Independent Contractor Requirements

In case that independent contractors or consultants is employed and is obliged to pass the backgroundcheck procedures. Any such contractor or consultant are only permitted to access to the CA's secure facilities if they are escorted and directly always supervised by trusted officers.

For system maintenance purposes, operating staffs must present their employee identification card to Trusted Persons for verification and record. They must be also escorted and directly supervised by trusted officers at all times.

Contractors fulfilling Trusted Roles are subject to all personnel requirements stipulated in thisGuidelines.

PKI vendors who provide any services must establish procedures to ensure that any subcontractors perform in accordance with this guideline and the CPS of the Certifying Authorities.

Independent CA services subcontractors and their personnel are subject to the same backgroundchecks as the CA personnel.

6 Documentation Supplied to Personnel

The Certifying Authority must provide its personnel the requisite documentation needed to perform their job responsibilities competently and satisfactorily. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

7 Job Rotation Frequency and Sequence

The Certifying Authorities shall specify the job rotation frequency and sequence of officers inits Certification Practice Statement.

8 Sanctions for Unauthorised Actions

8.1. Any Personnel, who fail to comply with the order of the Controller made under Information and Communication Technology Act, 2006, shall be punishable under Section 59 of the same Act.

8.2. Appropriate disciplinary actions are taken for unauthorized actions or other violations of relevant policies and procedures. Disciplinary actions are commensurate with the frequency and severity of the unauthorized actions and may include measures up to and including termination.

9 Qualifications, Experiences, Roles, and Responsibilities for Trusted CA Personnel

9.1. Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actionscorrectly or the integrity of the CA is weakened. The functions performed in these roles formthe basis of trust in the CA. The CA must take two approaches to increase the likelihood thatthese roles can be successfully carried out:

a) The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained; and

b) The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

9.2. Qualifications, Experiences, Roles, and Responsibilities of Trusted CA Personnel

Certifying Authority shall maintain the following qualifications and experience of the employees of the Certifying Authorities as per the section 19(c) of the Information and Communication Technology Act, 2006:

CA Senior Manager or any individual solely managing the CA operations

Qualification	• Must be a graduate in CS or CSE or Engineering • Must be proficient in Programing using Java, java scripts etc. (Optional) • Must have experience in developing API for data exchange (Optional) • Minimum 3 years of experience of CA operations is mandatory • Must have knowledge on local laws governing CA operations • Must have complete understanding on CPS document approved by CCA • Must have training or had subject on cybersecurity during BS level study
Training and certification	• Cybersecurity related areas • Personal Data Privacy • PKI management and implementation
Responsibilities	• Manage the whole CA operations • Prepare and update SOP, CPS, CP, User Manuals required for CA Operations • Prepare required reports for Controller of Certifying Authority • Arrange regular audit required by law governing CA and licensing guidelines • Arrange IT security audit to ensure security compliance of the system • Ensure security of all appliances, computer system and the CA infrastructure • Ensure reporting as required by the laws of the country • Timely renewal of all licenses of software, appliances for operation of CA • Ensuring timely renewals CA operating license

RA Manager or any post with similar responsibility

Qualification	• Must be a graduate in any area of IT or Physics or math or statistics from any University; or • A graduate with Post Graduate Diploma in IT from any university • Training on cybersecurity is desirable
RA Training	• Minimum 3 weeks intensive training by the employer on CA operations and functions of RA • Minimum 1 week training on use of tools, documentation
Responsibilities	Registration authority (RA) manager verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. RA cannot create or issue a certificate- as this is the sole responsibility of the CA- it works as an intermediary for the CA to collect necessary information and to process the following tasks: • receive user or device certificate requests; • validate users or devices;

	• authenticate users or devices; and • revoke credentials if the certificate is no longer valid. • Forwards the certificate request to the CA, to complete the digital certificate request process.

RA Operator or any(s) post with similar responsibility [No of Position: 1 or Multiple (as required)]

Qualification	• Must be a graduate in any area of IT or Physics or math or statistics from any University OR • A graduate with Post Graduate Diploma in IT from any university
RA Training	• Minimum 3 weeks intensive training by the employer on CA operations and functions of RA • Minimum 1 week training on use of tools, documentation
Responsibilities	• receive user or device certificate requests; • validate users or devices; • authenticate users or devices; and • Reports to RA manager if the certificate is no longer valid. • Forwards the certificate request to the RA Manager for reporting to CA, to complete the digital certificate request process; or • Forwards the certificate request to the CA, to complete the digital certificate request process. (if authorized by the CA)

Security Manager

Qualification	• Must be a graduate in CS or CSE or Engineering • Knowledge of network components, their operations and appropriate security controls and methods • Knowledge and experience of risk assessment, mitigation, and management methods. • Complete knowledge and understanding of regulatory requirement for cybersecurity, privacy. • 3 years' experience in managing cybersecurity and PKI implementations.
Training and certification	• Computer network operations and security • Cybersecurity related areas • Personal Data Privacy • PKI management and implementation
Responsibilities	• Read and interpret technical diagrams, specification, drawings, blueprints and schematics relating to systems and networks. • Determine and document security controls for systems and networks • Define and document the effect of the new implementation of new system or new interfaces between systems on the security posture of the existing environment • Recommend cost effective security controls to mitigate risks identified through testing and review. • Ensure cybersecurity risks are identified and managed appropriately through the organization's risk governance process. • Hardware Security Module (HSM) administration

Key Manager

Qualification	• Must be a graduate in CS or CSE or Engineering • Knowledge of PKI, Cryptography, cryptographic key management • Must have 3 years of experience in key lifecycle management of PKI
Training and certification	• Computer network operations and security • Cybersecurity related areas • Personal Data Privacy • PKI management and implementation
Responsibilities	• Management of all shareholders' keys, HSM security officers' keys • Track and maintain the lifecycle of keys of CA and Sub-CAs under the CA • Conduct Key generation ceremony • Plan and implement MofN user keys according to the CPS

Server/System Administrator

Qualification	• Must be a graduate in CS or CSE or Engineering • Knowledge of server, operating systems administration • Knowledge on Basic Networking
Training and certification	• Linux/Windows Administrator level training/certification • Operating System hardening training
Responsibilities	• Administer all CA operation related servers • Secure all operating system according to the industry standards • Maintain Auditing and logging of all systems according to the requirement of PKI Auditing Guidelines • Ensure backup of all systems and related data • Regular monitoring of system health and performance • Administer network and security devices • Storage Administration

Database Administrator

Qualification	• Must be a graduate in CS or CSE or Engineering • Knowledge of database administration
Training and certification	• Linux/Windows basic level training • Database administrator training/certification
Responsibilities	• Administer all database operation of PKI related services • Ensure high availability of database infrastructure and secure database infrastructure according to the industry standards. • Maintain Auditing and logging of all database systems according to the requirement of PKI Auditing Guidelines • Ensure backup of all data stored in the database • Regular monitoring of database health and performance

Support Engineers [No of Position: 1 or Multiple (as required)]

Qualification	• Must be a graduate in CSE or electrical and electronics engineering • Experience in system and solution support and trouble shooting • Training on ITIL is desirable.
Training and certification	• PKI related basic training
Responsibilities	• Ensure 24x7 support to the customer • Monitoring the entire CA systems and work as first responder for handling service request and incidents • Provide necessary customer on-boarding training • Support customer related to API integration with external Sub-CA or e-Sign business applications owner • Prepare regular report on CA system monitoring and service level agreement

In addition to the above responsibilities, the trusted personnel of the Certifying Authorities must follow the following principles regarding separation of duties-

- Responsibility of HSM MofN key shareholders shall not be performed by the Key Manager and Security Manager Role;
- HSM Security Officer Role shall not be performed by person performing Security Manager or HSM Administrator Role (e.g. Database Administrator can perform the role of HSM Security Officer);
- Single person cannot hold multiple roles mentioned in the note.
- Wherever applicable there can multiple persons in the roles.

10. Arbitration

In the event of any differences or dispute between the Certifying Authority and its personnel and failure to resolve the differences or disputes amicably among them, the Certifying Authority shall refer the matter to the Controller for resolution of the same. The decision of the Controller in that regard will be final and binding.

11. Savings

Any action taken, order passed or proceeding commenced by any Certifying Authorities for conducting any recruitment or appointments made under the provisions of any rules, regulations, policies or order in force immediately before the commencement of these Guidelines, shall, so far as they are not inconsistent with the provisions of these Guidelines be deemed to have been taken, passed, made or commenced as the case may by, under the corresponding provisions of these Guidelines.

12. Force Majeure:

Licensed CAs or their personnel shall not be liable for any failure or delay in their performance under this Guidelines due to causes that are beyond their reasonable control, including, but not

limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake,riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

13. Interpretations

These Guidelines shall be read and interpreted in conjunction with the appointment letter and in case of any controversy or ambiguity the decision of the Appointing Authority shall befinal and binding on all concerned.

14. Amendments

Office of the Controller of Certifying Authorities shall have the right to change, amend, modify, alter, rescind or delete any or all the Guidelines contained herein as may appear to him to be expedient for efficiently carrying on the operation of Certifying Authorities.

30.06.2024
এ. টি. এম. জিয়াউল ইসলাম
নিয়ন্ত্রক (যুগ্মসচিব)
ইলেকট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী
কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ