Leveraging ICT for Growth, Employment and Governance Project
Bangladesh Computer Council (BCC)
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
ICT Tower, Plot # E-14/X, Agargaon, Dhaka-1207
Bangladesh

Terms of Reference

For

CA Manager
(Contract Package #AF-S43A)
(Credit # 5911-BD)

July 2018

Terms of Reference (TOR)
For
CA Manager
(Contract Package #AF-S43A)

1. Objective of the Assignment

The objective of the assignment is to recruit a CA Manager for ensuring smooth operation and maintenance of Bangladesh Government Certification Authority (CA). The recruited CA Managers will be accountable for operations, maintenance and administration of the Government CA.

2. Scope of Services

Primary responsibilities associated with this role are:

- Lead a team of Public Key Infrastructure (PKI) subject matter experts to facilitate the operations of the Government Certification Authority (CA)
- Supervise staff, assignment of work, schedules, day to day workflow, and operating costs
- Achieve Public Key Infrastructure (PKI) operational objectives by contributing information and recommendations for new initiatives
- Maintain and/or improve implementation standards for current initiatives
- Maintain a high level of customer service standards to include maintenance and routine review of metrics and problem resolution and integrating with other teams when needed
- Achieve government's information security objectives by adhering to strict policy requirements while implementing operations, participating in annual audits, and change control boards.
- Technical program oversight specific to the PKI security domain
- Identify concepts and architectural areas of need specific to the PKI domain
- Manage the successful technical delivery of digital certificates and services for customers by working directly with key business stakeholders, executives and teams. Security architects are often the technical lead on initiatives and as such must drive the vision and alignment of the solution delivery.

Analytical/Decision Making Responsibilities:

Individuals in this role must be well versed and educated in common Information Security practices and the CISSP domains, as well as possess general Information Technology experience. They must be able to leverage these experiences and education to identify opportunities for improvement in the present information security architecture focusing on PKI, encryption, and certificate-based authentication solutions as well as furnish thought leadership around enacting the necessary improvements and addressing gaps.

Further, individuals must be able to meld key tenets of information security, through policy and best practices, to the IT strategies to develop technical security strategies that properly align. It is anticipated that Security Architects will work through their leadership to gain an understanding and perspective on emerging IT strategy as part of these efforts.

3. Knowledge, skills and experience requirements

Individuals are expected to have a strong background across all of the following information security domains, with industry expertise in, at minimum, one:

- Public key infrastructure
- Understanding of PKI Policy, Life Cycle management and Auditing of PKI Infrastructure
- Strong authentication / multi-factor authentication technologies
- Cryptographic services
- Data Protection
- Working understanding of Asymmetric & Symmetric Key Cryptography and Encryption /Hashing/ Digital Signatures

Further, the individual must be well versed in the practices and methods within IT Services, specifically:

- IT Strategy
- Enterprise Architecture

Individuals must possess leadership skills and capabilities commensurate managing professional relationships within a team, influence decisions based on data driven presentation and critical thinking, and the individual must have exceptional communication skills.

Preferred skills include:

- Expert level experience in MS Certificate Management Services and Active Directory Domain Services.
- Expert level experience in SSL certificate management concepts, processes, and solution management.
- Expert level experience with PKI implementation and certificate lifecycle management solution.
- Expert level experience with hardware security module (HSM) technology.
- Expert level experience in cloud solution development with Azure or AWS architectures as it related to PKI management.
- Minimum three (3) years of software development experience is desirable.

4. Education and Experience

- Minimum, Bachelor degree in Information Technology/ Computer Science/Computer Engineering (or similar)
- Minimum four (4) years' experience in PKI.
- One of CISA or CISM or CISSP certificate preferred

5. Reporting Arrangements

The CA Manager will assist and report to the Project Director, under the general supervision and guidance of the e-Government Team Leader and Technical Specialist(s).

6. Duration of the Assignment:

The duration of the assignment will be about 10 (ten) months and may extend subject to satisfactory performance of the Consultants & Project Extension.

7. Facilities to be provided by the Client:

Project will provide appropriate office space and other associated (data, information, furniture, stationeries, etc.) necessary to carry out the assignment.

8. Reporting requirements/deliverable:

The CA Manager will need the following reporting requirements/deliverables, but not limited to:

- Monthly work plan and progress report;
- Yearly Report;
- Any other Report, as required.