Terms of Reference (ToR)
for Development of eKYC System for BCC e-Sign Service

1. Background

Bangladesh Computer Council Certification Authority (BCC CA) is the only government CA amongst 6 licensed CA in Bangladesh. Since its inception, BCC CA has been working continuously to issue digital certificates to citizens and help integrate Public Key Infrastructure (PKI) services specially digital signing services. Before issuing a digital certificate, BCC CA has to manually verify a person`s identity. BCC intends to introduce e-kyc system for their customer`s identity verification purposes, which has the potential to drastically reduce the time for issuing a digital certificate to the subscriber.

1.1 About the Organization

Bangladesh Computer Council (BCC) under ICT Division is the apex ICT agency of the government towards materializing the Digital Bangladesh vision of the government. Apart from developing ICT infrastructure, capacity development, BCC is also working to support the government to ensure information security and promote e-governance. One of the initiatives that have been taken by BCC is to operate as one of the licensed Certification Authority (CA) under the ICT Act 2006 to issue digital signature certificate for the citizens/agencies. BCC wants to revamp the certificate issuance process so that it can be scaled to delivering certificates to tens of millions of citizens.

1.2 Existing Service

For issuing any certificate a user has to fill-up an online enrollment form, where he gives all his details for KYC(Know Your Customer) purpose. After that, a verification authority from BCC CA used to verify customer`s provided details and identity. This verification process is done completely by a human operator. Hence, it takes time to onboard new customers.

1.3 Problems and Challenges

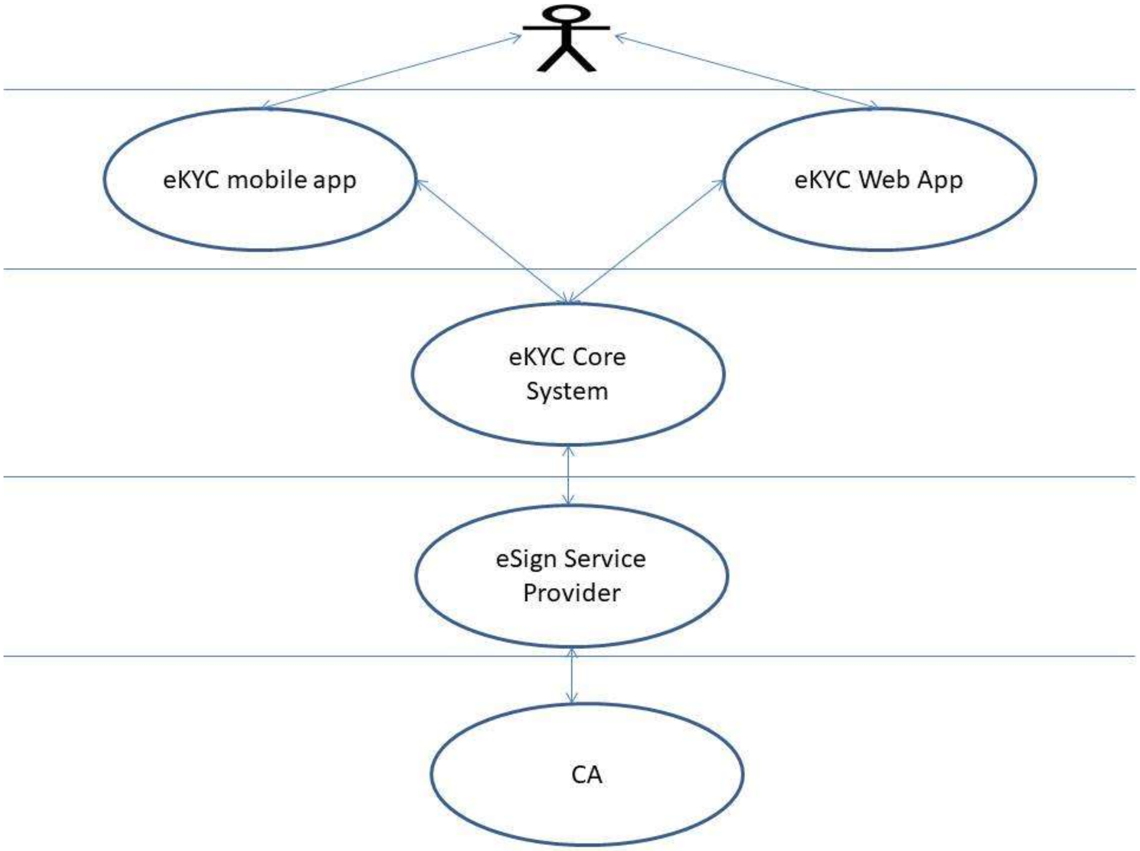
The process of manually verifying customer`s kyc details- is slow and it cannot be scaled to serving millions of citizens. This is a significant challenge in rolling out public key infrastructure and digital-signature to mass people.

2. Objectives

According to the guideline provided by Office of the CCA, BCC intends to extend the digital signing services by introducing e-Sign (remote signature) service for the customer. BCC desires to automate the KYC process in a way that the whole KYC verification process will be done electronically and automatically to issue e-Sign service to the subscriber. The key objective is quick onboarding of customers by verifying customer identity through digital means which can leverage saving of time and provide ease both for the client and BCC CA. The faster onboarding/verification of a customer should transform the issuing of the more and more certificates. Additionally, e-KYC can save institutional costs as well as foster growth of customer base compared to the traditional growth.

3. Brief Requirement of the System

According to the following component architecture of the systems, below is the requirement (not limited to) for the eKYC system:



3.1 eKYC Core System

1. eKYC core system shall be connected with the eKYC subsystems(eKYC mobile & Web App) and it shall be able to integrate to esign Service Providers Service with API.

a) Core system shall have a customer management module which shall consist of atleast following:
   a. customer enrollment
   b. profile management
   c. device enrollment for authorization
   d. customer authentication & authorization
   e. customer dashboard
   f. notification management
   g. customer support

    h. search feature etc.

b) Core system shall have user management module(eg: admin, operator, manager, super admin etc). User shall have following functions:
    a. user management
    b. customer management
    c. customer support management
    d. report management
    e. ESP API management
    f. User Authentication Management.
    g. Agent Management

2. The core eKYC system shall have an agent module for biometric enrollment of customer for advanced esign.
3. The core eKYC system shall be able to integrate with the following external services:
   a) NID Database
   b) SIM Registration database(optional)
   c) ESP's Esign API
   d) Identity Management System(e.g. LDAP/AD etc)
   e) eKYC subsystems(eKYC mobile and web app)
   f) SMS gateway
   g) SMTP Gateway
4. The core eKYC system should have biometric (face and fingerprint) matching module with following minimum feature:
    a. The core eKYC system shall have the verification capability for Face Matching from both Paper Based/Smart NID photo.
    b. The core eKYC system should produce both summarized & detailed verification results & scores for each component (e.g. face-matching, demographic data etc) should be available in accordance with CCA esign guideline.
    c. The core eKYC system's False Acceptance Rate (FAR) for Facial Matching needs to be equal or lower than .01%.
    d. The face matching system should be deployed on premise by developing and training the model.
    e. the capacity for verification through captured Fingerprint and should be able to integrate with Election Commission API for fingerprint matching when it's available according to the guideline.
5. The core eKYC system shall have a system for automatic population of bilingual (Bangla & English) alphanumeric data fields related to NID Card (Smart/Paper Based) by automated information extraction through OCR (Bangla & English).
6. The core eKYC system shall expose API so that eKYC subsystems(eKYC mobile and web app) can consume the API.
7. Customer can register from mobile/web based eKYC app and can login using the same account information from any device.
8. The core eKYC system shall have a Notification module to send push (to ekyc mobile app), SMS and email notification .

9. The core eKYC system shall have a O&M module. This module shall have provision to monitor the health/status of different subsystems. It shall also send alerts or notify the administrators when any submodule is not functioning as expected .
10. The core eKYC system shall have capability to generate event based logs as required.
11. The core eKYC system should allow for printing and downloading of the filled-up form along with uploaded documents.
12. The core eKYC system should have the availability of Two-factor Authentication (eg: SMS OTP, TOTP etc) login/authentication system for users.
13. Upon successful verification, the core eKYC system should communicate with e-sign system and send the user detail(email,phone number,name,nid etc.) to e-sign system(esp), for which certificate will be issued.

3.2 ekyc Mobile App

1. The eKYC mobile app shall be developed to operate on both for android and ios platform.
2. The eKYC mobile app shall prompt the customer to login or to register.
3. The following inputs for registration shall be required by the eKYC mobile app for basic e-Sign:
   a) Front and rear side of NID(Smart/Paper Based)
   b) Live Selfie
   c) Mobile Number
   d) Email Address.
4. According to CCA eSign guideline, an user can request to upgrade from basic eSign account to advanced eSign by providing following information to the authorized agent:
   a. Fingerprint
   b. Mobile Number/User ID
5. The mobile app shall be able to send all the customer data securely to eKYC core system.
6. Upon successful verification(biometric & demographic) by the eKYC core system, the customer will be prompted for submitting OTP sent to the provided mobile number.
7. If the OTP is correct the customer shall be asked to set his secure PIN. After setting the PIN, customer shall be notified about successful registration.
8. If the OTP is incorrect the customer will be provided with an option to resend OTP.
9. Upon failed verification(biometric & demographic) by the eKYC core system, the customer will be notified about the failure.
10. Upon successful registration, user can login to the app using their user id/mobile number and pin.
11. User can manage profile, view dashboard, access support, request to upgrade profile to advanced esign , setup device for authorization, activate email etc.
12. For setting up device for authorization, as well as for authorizing a signing request using ‘device authorization’ – the mobile App has to integrate with mobile SDK of ESP.

3.3 ekyc Web App

1. The eKYC web app shall be developed to operate on all modern browsers and should be w3c compliant. The web apps must be responsive on all devices (desktops, tablets, and phones)
2. The eKYC web app shall have the option for customer to login or to register.

3. The following inputs for registration shall be required by the eKYC web app for basic e-Sign:
   a) Front and rear side of NID(Smart/Paper Based)
   b) Live Selfie(from webcam)
   c) Mobile Number
   d) Email Address
4. According to CCA eSign guideline, an user can request to upgrade from basic eSign account to advanced eSign by providing following information to the authorized agent:
   c. Fingerprint
   d. Mobile Number/User ID
5. The web app shall be able to send all the customer data securely to eKYC core system.
6. Upon successful verification (biometric & demographic) by the eKYC core system, the customer will be prompted for submitting OTP sent to the provided mobile number.
7. If the OTP is correct the customer shall be asked to set his secure PIN. After setting the PIN, customer shall be notified about successful registration.
8. If the OTP is incorrect the customer will be provided with an option to resend OTP.
9. Upon failed verification(biometric & demographic) by the eKYC core system, the customer will be notified about the failure.
10. Upon successful registration, user can login to the app using their user id/mobile number and pin.
11. User can manage profile, view dashboard, access support, request to upgrade profile to advanced esign , activate email etc.
12. Users registered through web app shall be able to login with mobile app when needed.

3.4 ekyc Mobile App(Agent)

1. The same ekyc Mobile app shall be used by the agent to login however agent shall be prior registered through web app.
2. The agent will take customer mobile number and verify that the customer is registered for basic esign.
3. If the customer is already registered, agent shall enroll the customers fingerprint for upgrading to advanced esign.
4. BCC recommended fingerprint reader shall be integrated with the app for capturing fingerprint data. Proper security measures(according to the guidelines of Bangladesh Election Commission) must be taken to transmit this fingerprint data to ekyc core system .

4. Design, Development & Implementation Requirements

1. Solution architecture should be based on 3-Tier web based Architecture
2. The solution should be highly scalable, robust
3. The system should be inbuilt with load management functionality
4. System internal architecture should support high availability
5. The application architecture preferably in distributed and microservice architecture
6. Platform independent solution will be given preference
7. Maintain SOLID principles and SDLC methodology preferably Agile
8. Must follow clean and quality code

9. Automate CI/CD pipeline for building, testing and deployment using opensource tools
10. The application has to be cloud native. Provide necessary scripts to deploy the system using docker container and Kubernetes.
11. Comply with all the industry best practices for securing mobile and web application (eg: OWASP secure coding practices)

5. Scope of Work

The scope of the work for the system is as below:

- Requirement analysis as per the provided brief requirement;
- Prepare and finalize business requirement specification(BRS)
- Prepare detailed software requirement specification (SRS) according to the format accepted by Software Quality and Testing Center (SQTC), BCC.
- Prepare and finalize Functional Requirement Specification(FRS)
- Prepare the high level(architectural) and low level design.
- Prepare detailed work plan and staffing plan for the system development;
- Demonstrate with mock/dummy UI on the whole system;
- Get approval on each major step of the development lifecycle from BCC;
- Develop and Test the software system;
- For ensuring complete visibility on the development cycle, development of the entire system shall be carried out using BCC's own code repository;
- Independent test has to be carried out from SQTC, BCC;
- Provide system deployment architecture to BCC;
- Assist in deployment of the final system in BCC National Data Centre ;
- All future bug fixing/changes/improvement shall be applied from git repository which will be under full control of BCC;
- Proper knowledge transfer to BCC.
- Provide communication and escalation matrix;
- Provide maintenance and improvement support for 3 Years according to the agreed Service Level Agreement (SLA);
- Any other scope that may be deemed necessary by BCC during finalizing the ToR.

6. Expected Deliverables

Following are the list of deliverables (not limited to):

- Project inception and management report
- Business requirement specification (BRS)
- System requirement specification (SRS)
- Functional requirement specification (FRS)
- System design document (SDD)
- ER Diagram
- Complete source code
- All test cases and test scripts

- Training plan and reports
- Training materials and user manuals
- Total eKYC system eKYC Core System
- Mobile Application (Android & iOS)
- Web application
- UAT Report
- Maintenance, agreement & SLA
- Deployment Manuals

7. Staffing Requirement

Following are the minimum staffing requirement:

SL	Title	Qty.
1	Project Manager	1
2	Solution Architect	1
3	Devops Engineer	1
4	System analyst	1
5	Database Administrator	1
6	Senior Software Engineer	2
7	Software Engineer	4
8	UI/UX Designer	1
9	QA Engineer	2
10	Support Engineer	2

8. Duration of the Assignment

The duration of the assignment is 6 (Six) months after signing the contract excluding the maintenance and support service period.