CENTRAL DEPOSITORY AND SETTLEMENT CORPORATION

REQUEST FOR PROPOSAL (RFP) FOR DEVELOPMENT OF AN APPLICATION PROGRAMMING INTERFACE

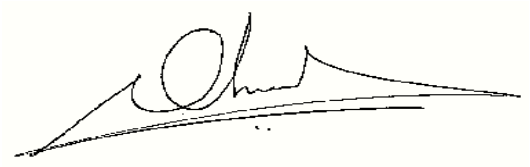
SEPTEMBER 2020

Release Date **: 9th September 2020**

Last Date for Submission of responses **: 30st September 2020** **Time 1400hrs EAT**

CDSC invites you to submit your proposals for development of an application-programming interface. The bids shall consist of one soft copy (PDF) sent on email rfp@cdsckenya.com and another soft copy may be delivered at CDSC on Compact Disc (CD) or USB in case of email issues/challenges.

Yours Faithfully



Nkoregamba Mwebesa

CHIEF EXECUTIVE OFFICER

1 Table of Contents

1 INTRODUCTION

The Central Depository & Settlement Corporation Limited (CDSC) is a limited liability Company approved by the Capital Markets Authority to provide automated Depository, Clearing, and Settlement services in respect of transactions carried out at Nairobi Securities Exchange as well as holding of listed and non-listed securities including other documents of title on behalf of investors.

2.1 Purpose

The purpose of this Request for Proposal (RFP) is to solicit proposals for the development of an Application Programming Interface (API) to allow Central Depository Agents' (CDAs) Systems to integrate with the CDSC Central Depository System (CDS). CDSC requires that the existing CDS functions be exposed to the CDAs by APIs. The API will make use of the existing configurations, validations, notifications, and Multi-Step Approvals (MSA).

2 GENERAL SUBMISSION REQUIREMENTS/INSTRUCTIONS TO BIDDERS

2.1 Completion and Submission of the RFP

a) From the information and details on the following pages, a proposal document should be prepared, as the RFP response consisting of one soft copy (PDF) sent on email (rfp@cdsckenya.com) and another soft copy may be delivered at CDSC on Compact Disc (CD) or USB in case of email issues/challenges.

b) The bids should be submitted on email and a Compact Disc (CD) / USB labeled **"APPLICATION PROGRAMMING INTERFACE**" to the CEO by **30th September, 2020** before 2:00 pm.

c) The following proposals are required and should be appropriately labeled as: -

The Administrative requirements - the Overview and profile of the company including the management structure, details of company directors, the CEO, Project leader and Project team, confidential business questionnaire.

- Attach a copy of Certificate of incorporation/registration **(MANDATORY).**
- Attach a Copy of KRA Pin certificate **(For local bidders only) (MANDATORY).**

- Attach a Copy of current Tax Compliance Certificate **(For local bidders only) (MANDATORY).**

The Technical Proposal – An Application Programming Interface proposal seeking to demonstrate relevant competency and expertise to cover the items in section five.

The Commercial proposal – Indicating all the details of pricing.

3 REQUIREMENTS

3.1 Requirement Brief

The RFP response is to consist of -

Administrative requirements

- This RFP document duly signed

A Company profile in the following format: -

- A brief Introduction - This is a summary of your company history, accomplishments, philosophy and experience on similar assignments in the financial sector.
- Owners, Directors and CEO of the company submitting the RFP bid.
- A copy of Tax Compliance Certificate (For Local Bidders only)
- A copy of KRA Pin certificate (For Local bidders only)
- A business registration or Incorporation certificate
- Confidential Business Questionnaire (Appendix 1)

CR12-The official confirmation by the Registrar of Companies in Kenya as to who the directors/shareholders of the company are. To also confirm that the company's records exist at the Company registry **(For local bidders only) (MANDATORY).**

Technical Proposal: The write up of the proposal should cover the technical aspects as outlined below; Demonstrate understanding of our requirements on how the firm will meet our requirements, covered in section five. This entails the knowledge and interaction with CDS and CDA systems and operations.

- The experience of the firm with regards to provision of similar services. The firm should provide a list of reference sites where they have developed APIs evidenced by Actual signed letters (scanned and appended or otherwise) of recommendations from at least 3 clients for similar projects completed successfully should be provided.
- Number of technical personnel and their qualifications. This should include the proposed team leader and the team that will develop the API the team MUST attach Copies of qualification certificates for the personnel that will be involved should be attached.
- Proposed methodology and work plan. This entails a detailed plan of Information Gathering, developing, testing and implementing the API.

Financial proposal –

The single currency for price conversions is **Kenya Shillings**

The source of official rates is **Central Bank of Kenya**.

The date of exchange rates is **Last Date for Submission of responses**

3.2 Evaluation Criteria

3.2.1 Method of Award

The evaluation of each response to this RFP shall be based on its demonstrated competence, compliance, format, and organization.

Preliminary Evaluation

Your proposal will be assessed based on the following evaluation criteria: -

Mandatory Requirements

	A. PRELIMINARY EVALUATION	MANDATORY
1.	Certificate of Incorporation/ Business registration	**YES**
2.	Filled Confidential Business Questionnaire (Appendix 1 -KYC)	**YES**
3	KRA Pin certificate (For Local bidders)	**YES**
4	Valid Tax compliance certificate (For Local bidders)	**YES**
5	Valid CR 12 certificate	**YES**

Technical Evaluation
Evaluation Criteria: Technical Evaluation

N0.	TECHNICAL SCORE	SCORE
1	**Completeness of the proposal in regards to satisfying CDSC requirements. (35 Marks)** • Company profile **(5 mks)** • The bidder should demonstrate the understanding of functional requirements in Section V below and understanding of CDS operations providing a detailed Project Schedule, of Information gathering, developing, testing and implementing the API methodology, work plan, resource allocations, deployment, implementation, training and hand over and provide comments and any add-ons on our RFP **(30 mks)**	**35**

2	**General qualifications of the Project lead and key staff to be involved in deployment and implementation of the API (35 Marks) (**Each member of the team shall ensure his/her availability during the duration of the assignment) Project Lead to undertake the assignment - Details of academic and professional qualification of key consultant to be involved in the project. The Project Lead should have a minimum of • University Degree-5 points • Relevant professional qualification/Certification—5 points • Over 5 years' experience covering areas in scope or similar deployments-10 points. If Less than 5 years' experience or similar deployments -5 points At least two other proposed key staff to undertake the assignment. Project team members (2 other proposed members) • University Degree-5 points • Relevant professional qualification/Certification—5 points • Over 3 years' experience covering areas in scope or similar deployments-5 points. If Less than 3 years' experience covering areas in scope or similar deployments -2.5 points (An average score of the team members will be taken and awarded) (Provide evidence of qualification and experience by attaching CVs and copies of academic and professional certificates for the Project lead and other proposed team members.)	**35**
3	**Specific Firm Experience in deployment of API or similar projects (30 mks)** • Experience. Evaluation of the experience in covering deployment of API or similar projects. Recommendation letters from three clients indicating successful completion of similar project. If you have less than three clients, you will get 10 points per client. (Supporting evidence shall be Actual signed letters of completion/LPO/LSO, Contracts, Recommendation of similar projects done in the past from past clients or fill in the firm reference template **Appendix 2 below** and have it **stamped and signed by the referring firm/Past Client**	**30**
	Maximum Technical Score	**100**
	Minimum Pass Score out of 100	**80**

3.2.2 Additional evaluation details

The technical evaluation will constitute of 80% of the overall rating and will include the analysis of the technical responses based on the write up and documents submitted.

Financial evaluation

Financial evaluation will be done independently and will constitute of 20% of the overall rating. Financial evaluation will be based on adherence to general contract conditions.

Detailed Cost Schedules:

Provide detailed, itemized unit and total costs for each component and service proposed, indicating as appropriate optional and required components and services.

Tender Validity: the proposal and quote should have a validity of 150 days

Detailed Evaluation

The responsive proposal with the highest score determined by CDSC by combining, for each proposal, in accordance with the procedure and criteria set out in the request for proposal. The scores shall be assigned to the technical and financial proposal. Combining financial and technical score will be carried out as follows; the weight to be assigned for technical score (t) will be 80% while the financial score (p) will be 20%. The bidders with the highest combined financial and technical score (t+p) will be invited for negotiation.

3.2.3 Selection and Notification

Consultants determined by CDSC to possess the capacity to compete for this contract will be selected to move into the negotiation phase of this process. Written notification will be sent to these Consultants via mail. If you do not hear from us within 60 days of closure of this RFP, please consider your response/submission unsuccessful.

4 API REQUIREMENTS

Functional Requirements

Account Registration View: This functionality will include an API to look-up information on a specified registration. A registration number will be passed in the request. Validation will be carried out on the request, and the requesting CDA. A response will be provided to the CDA via the API, containing information on the investor registration.

Holdings Detail View: This functionality will include an API to look-up information on a specified registration's holdings. A registration number will be passed in the request. Validation will be carried out on the request, and the requesting CDA. A response will be provided to the CDA via the API, containing information on the investor registration holdings that include the various applicable balances.

New Account Opening: This functionality will provide the CDAs the ability to open investor accounts on the CDS application, through an API. The existing data and document validations configured in CDS will apply. A system generated response will be sent to the requesting CDA through the API. The Multi Step Approval (MSA) workflow configured in the CDS will be applied and used for the account opening i.e. approval notifications will be sent to permitted users for authorization. The existing Sybrin document storage services will be exposed to the CDAs for this function.

New Account Registration: This functionality will provide the CDAs the ability to open investor registrations on the CDS application, through an API. The existing data and document validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The MSA workflow configured in the CDS will be applied and used for opening the registration i.e. approval notifications will be sent to permitted users for authorization. The existing Sybrin document storage services will be exposed to the CDAs for this function.

Account Statement Request: This functionality will provide the CDAs the ability to request an investor's registration statement. The CDA will have the ability to select the statement format

(pdf or xls). The existing validations will be applied, including the checking of an investor's email address. A system-generated response will be provided to the CDA via the API. The CDS application will generate the investor's statement in the specified format and send it to the investor's email address.

Static Details Amendments: This functionality allows the CDA to amend static details pertaining to the investor. This functionality will provide the CDAs the ability to amend investor accounts on the CDS application, through an API. The existing data validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The MSA workflow configured in the CDS will be applied and used for the amendments i.e. approval notifications will be sent to permitted users for authorization.

Pledging: This functionality allows the CDA or any financial institution e.g. banks to request a pledge on the investor registration through an API. The existing data validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The multi step approval (MSA) workflow configured in the CDS will be applied and used for pledges i.e. approval notifications will be sent to permitted users for authorization.

Freezing: This functionality allows the CDA or any financial institution e.g. banks to request a freeze on the investor registration through an API. The existing data validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The MSA workflow configured in the CDS will be applied and used for freezes i.e. approval notifications will be sent to permitted users for authorization.

Transfers: This functionality allows the CDA to request a transfer from one investor registration to another through an API. The existing data validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The MSA workflow configured in the CDS will be applied and used for transfers i.e. approval notifications will be sent to permitted users for authorization.

Dormancy Lifting: This functionality allows the CDA to lift the dormancy status of an investor registration through an API. The existing data validations configured in the CDS will apply. A system generated response will be sent to the requesting CDA through the API. The MSA workflow configured in the CDS will be applied and used for the amendments i.e. approval notifications will be sent to permitted users for authorization.

Trade Information: This functionality allows the CDA to request trade information on an investor's registration through an API. The existing validations in the CDS will be applied to the request. Trade information will be sent to the CDA via the API on successful validation.

Request Enquiry: This functionality allows the CDA to query the CDS application for the outcome of their previously submitted request. This API will make use of the request reference number as the search criteria.

Non-Functional Requirements

The developer shall ensure **security** has been integrated in the development of the API. In addition to a secure API architecture design, the developers shall also ensure to include performance considerations in the design. The security requirements include addressing the top 10 open web application security project (OWASP) vulnerabilities. These are;

Broken object level authorization

Ensuring proper authorization checks to protect against attacks such as IDOR (Insecure Direct Object Reference).

Broken authentication

Ensure proper API authentication to prevent attackers from assuming other users' identities.

Excessive data exposure

Protect the API against exposing more data than what the client legitimately needs.

- ✓ Review all API responses and adapt them to match what the API consumers really need.

- ✓ Carefully define schemas for all the API responses.
- ✓ Error responses, define proper schemas as well.
- ✓ Enforce response checks to prevent accidental leaks of data or exceptions.

Lack of resources and rate limiting

Protect the API against an excessive amount of calls or payload sizes. Attackers can use this for Denial of Service (DoS) and authentication flaws like brute force attacks.

Broken function level authorization

- ✓ Do not rely on the client to enforce admin access.
- ✓ Deny all access by default.
- ✓ Only allow operations to users belonging to the appropriate group or role.
- ✓ Properly design and test authorization.

Mass assignment

- ✓ Do not automatically bind incoming data and internal objects.
- ✓ Explicitly define all the parameters and payloads you are expecting.
- ✓ Use the read only property set to true in object schemas for all properties that can be retrieved through APIs but should never be modified.
- ✓ Precisely define the schemas, types, and patterns you will accept in requests at design time and enforce them at runtime.

Security misconfiguration

Ensure proper configuration of the API servers to prevent attackers from exploiting them.

- ✓ Disable unnecessary features.
- ✓ Restrict administrative access.
- ✓ Define and enforce all outputs, including errors.
- ✓ Use secure communication channels that allow for end-to-end encryption
- ✓ Avoid outdated or misconfigured TLS.

Injection

Attackers construct API calls that include SQL, NoSQL, LDAP, OS, or other commands that the API or the backend behind it blindly executes.

- ✓ Strictly define all input data, such as schemas, types and string patterns.
- ✓ Validate, filter, and sanitize all incoming data.

✓ Define, limit and enforce API outputs to prevent data leaks. **Improper assets management**

Attackers find non-production versions of the API (for example, staging, testing, beta, or earlier versions) that are not as well protected as the production API, and use those to launch their attacks.

Logging and monitoring

Ensure proper logging, monitoring and alerting to allow attacks and attackers to be noticed.

- ✓ Log failed attempts, denied access, input validation failures, or any failures in security policy checks.
- ✓ Ensure that logs are formatted so that other tools can consume them as well e.g. SIEM
- ✓ Include enough detail to identify attackers.

APPENDIX 1 - KYC

CONFIDENTIAL BUSINESS QUESTIONNAIRE FORM

You are requested to give the particulars indicated in Part 1 and either Part 2(a), 2(b) or 2(c) whichever applies to your type of business. NB. Registration/Tax /PIN certificates, Trade Licenses SHALL be attached with form when submitting quotation.

Part 1 - General:

Business Name .....

Location of Business Premises .....

Plot No. ..... Street/Road .....

Postal Address ..... Tel. No. .....

Nature of Business .....

Current Trade License (from a Local Authority) No. ..... Expiring Date .....

V.A.T No…….

ETR No……

Tax Compliance Certificate No…….. Expiring Date……

Maximum value of business which you can handle at any one time: Kshs.....

Name of your bankers ..... Branch .....

Part 2 (a) Sole Proprietor:

Your name in full .....Age .....

Nationality .....…. Country of origin .....

Citizenship details .....

Part 2 (b) Partnership

Give details of partners as follows:

	Name	Nationality	Citizenship Details	Shares
1.				
2.				
3.				

Part 2 (c) Registered Company:

Private or public .....

State the nominal and issued capital of the company: -

Nominal Kshs .....

Issued Kshs .....

Give details of all Directors as follows: -

	Name	Nationality	Citizenship Details	Shares
1.				
2.				
3.				

APPENDIX 2

a) **Firm's References Template**

Relevant Services Carried Out in the past that Best Illustrate Your Qualifications

Using the format below, provide information on each assignment for which your firm either individually, as a corporate entity or in association, was legally contracted.

Assignment Name: Country	
Location within Country:	No of Professional Staff provided by Your Firm/Entity(profiles):
Name of Client:	Clients contact person for the assignment.
Address:	No of Staff-Months; Duration of Assignment:
Start Date (Month/Year):	Completion Date Approx. Value of Services (Kshs) (Month/Year):
Name of Associated Consultants. If any:	No of Months of Professional Staff provided by Associated Consultants:
Name of Senior Staff (Project Director/Coordinator, Team Leader) Involved and Functions Performed:	
Narrative Description of project:	
Description of Actual Services Provided by Your Staff:	

PAST REFEREE OFFICIAL USE ONLY

The details below should be completed, signed and stamped by the **Past Client** mentioned above

Firm's Name: _____

Name and title of Authorised signatory; _____

Signature; _____

Stamp of the Firm; _____