



**THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY
KENYA DIGITAL ECONOMY ACCELERATION PROJECT
ICTA-PROGRAM IMPLEMENTATION UNIT**

Name of Assignment: Supply, Delivery and Configuration of Additional Digital Signature Certificates on the Existing System Deployed for the Kenyan National Public Key Infrastructure (NPKI) and Government Certification Authority (GCA)

RFB Reference No.: KE-ICTA-482245-GO-RFB

Loan No./Credit No./Grant No.: IDA 7289-KE and 7290-KE

Country: Kenya

Date: 23th July, 2025

Dear Mr/Mrs:

RE: CLARIFICATION OF RFB DOCUMENT THROUGH CLARIFICATION 1

In accordance with the Instructions to Bidders [*Clarification of Bidding Document/ Technical Specification*], the Client is clarifying on Technical Requirement of the issued RFB Document

S/N	FP REQUIREMENT/SECTION REFERENCE	BIDDER'S CONCERNS/OBSERVATIONS/COMMENTS	CLARIFICATION/ RESPONSE
1.	Technical Specification/ Requirement	This project requires “Additional Digital Signature Certificates” to be issued which means the mentioned Government CA has already issued some number of certificates for some period of time. Can you please indicate launch date of the mentioned Government CA and the total number of the issued certificates?	The current CA was launched in 2022. The total number of Issued Certificates should not matter as what we require are additional Digital Certificates as defined in the RFP.
2.		The bid document says “The organization should provide proof of a robust Certificate Lifecycle Management and Organizational proof for secure and reliable certificate repositories...” but “certificate lifecycle management” and “certificate repository management” are the direct functions of CA. Does this means that the existing CA has no automation and the bidder is requested to install CA automation	The current setup is fully equipped to handle the certificate Lifecycle. The Bidder is not required to install any more additional applications.

	application for issuing certificates and for their management?	
3.	Does “Existing System Deployed for the Kenya National Public Key Infrastructure (NPKI) and Government Certification Authority (GCA)” include USB e-Token personalization workplaces including personal computers, appropriate software application for personalization and office equipment? How many USB e-Token personalization workplaces available and what is the maximal daily personalization capacity of each workplace? Is bidder requested to provide e-Token personalization application or develop new one?	No new applications are integration is required. It has e-token functionality personalization in built.
4.	How we can get CP and CPS documents of the” Existing System Deployed for the Kenya National Public Key Infrastructure (NPKI) and Government Certification Authority (GCA)” with the description of certificate issuing process beginning with the user certificate request?	The Regulations and framework documents that support the use of NPKI are available at https://govca.icta.go.ke/laws-regulations . The include; <ul style="list-style-type: none"> • Certificate Policy (CP) • Certificate Practice Statement (CPS) • Subscriber Agreement • Registration Authority Charter • Manuals & User Guides
5.	If the Government CA functions under some automation application can the bidders get manuals of this application or bidders requested to install (or develop) new CA application?	The link for the manual guide is as indicated below; https://govca.icta.go.ke/laws-regulations - Manual Guides.
6.	If the new CA application is required the bidders should know the type of computer servers and HSMs (hardware security modules) included into the hardware infrastructure. Please provide description of hardware infrastructure where new CA application should be installed.	The request does not require a CA application.
	According to the bid documents it’s expected that the bid winner will provide services on certificates issuing using existing infrastructure. Can you please indicate:	The Current PKI is based on the Nexus NPKI Core System.
7.	Does the existing CA has Registration Authorities (RA) for collecting user certificate requests. How many RAs and in which cities are they already deployed?	Yes it does. The Registration Authorities (RA) are many (Over 10) with potential for scaling with different tenants per entity.
8.	Which documents should be provided to accept user’s certificate request according the legislation?	Refer to the Document repository and Subscriber Agreement and Registration Authority Charter available at https://govca.icta.go.ke/laws-regulations .
9.	Are users allowed to generate asymmetrical key pairs or generation of these pairs will be done by RA (registration authority) operators?	Will be done by RA

10.		How many CA and RA operators does have the Government CA today? Is bid winner will be requested to provide these personnel or the bid winner should only manage and supervise the existing personnel for issuing e-certificates?	They will not be required to interact with either. The role of the bidder is to only provide the additional signatures to the current infrastructure.
11.		How many minutes in average take preparation of one user certificate request in RA?	Less than half a minute.
12.		What is the accepted USB e-Token certificate delivery method of existing Government CA?	encrypted USB tokens
13.		Does the exiting CA provide Application Program Interface (API) for integration? Is it possible, for example, to send PKCS10 type requests to CA API and get ready X509 e-certificate back? Can you please provide description of this API?	Yes it does provide APIs for integrations. This you can get from the Nexus website under CA solution
14.	DSC Integration Requirement	<p>The RFP specifically requires token-based (dongle-based) DSC integration, not Aadhaar-based e-Signing. Our current CA license supports only Aadhaar-based e-Sign, which may not align with this requirement.</p> <p>Vender Query: Can we onboard a CA partner who supports dongle-based e-Signing to fulfill this requirement?</p>	The specifications as per the RFP demonstrates and communicates the current system that we have and the required Digital Certificate Signatures Requirement. All vendors and provider should endeavor to fulfill the specification as requested. Onboarding of other vendors that amounts to Joint ventures is not Allowed as per ITB 4.1, unless there is other onboarding process.
15.	CA Certification (EAL4+)	<p>The RFP mandates that the Certifying Authority (CA) must be compliant with international standards such as Common Criteria EAL4+ and others.</p> <p>Vendor Query: If we are allowed to partner with another CA, would their EAL4+ and other certification will be acceptable to meet this requirement?</p>	If the partnering referred to in this case amounts to JV then it's not allowed as per ITB 4.1
16.	Local Licensing Requirement		An Authorized CA from another Cacan submit. However, they have to provide validation of their CA licenses.
17.	ITB 4.1	<p>The maximum number of members in a Joint Venture (JV) shall be: NONE</p> <p>Due to complexity of the requirements and request you to allow Joint Venture (JV)</p> <p>Due to the complexity of the requirements request you to extend the submission date by at least by two week so that we can provide the comprehensive solution v Due to the project's sensitivity (Digital Signatures), we won't allow Joint venture for this exercise.</p>	Due to the project's sensitivity (Digital Signatures), we won't allow Joint venture for this exercise.
18.	ITB 22.1	Submission Deadline	Due to the projects sensitivity(Digital Signatures), we won't and the timelines requirements, we wont allow for submission

This Clarification 1 forms part of the issued RFB document. All other terms and conditions of the issued RFB document remain unchanged.

Zilpher Owiti, OGW
Chief Executive Officer,
Information and Communications Technology Authority