National Internet Exchange of India

9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001

Request for Proposal (RFP)
For

Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers.

RFP No: **CCA/02(1)/2023-NIXI**

REF: **F.No. NIXI/CCA/02-2023**

Schedule for Invitation of RFP

Tender No.	**CCA/02(1)-2023-NIXI**
Published Date	22-03-2023
Clarification Start Date/Time	23-03-2023
Clarification End Date/Time	29-03-2023
Pre-bid Meeting	03-04-2023
Clarification Uploading & Amendment in RFP, (if any)	10-04-2023 (Tentative)
Proposal Submission Start Date/Time	12-04-2023@ 10:00 hrs.
Proposal Submission End Date/Time	18-04-203@ 15:00 hrs.
Proposal Opening Date/Time	18-04-2023@ 15:30 hrs.
Proposal Validity	75 days from due date of submission
EMD	Rs 20 lakhs/- (Rupees Twenty lakhs Only) in the form of DD drawn on Nationalized/Scheduled bank in favor of National Internet Exchange of India
Duration of PBG required (Months)	66 months PBG 5% of Bid Value
Minimum Average Annual Turnover (Last 3 yrs.)	75 Crores
Ministry	Ministry of Electronics & Information Technology
Organization Name	NIXI
Item Category	Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers.
Address of RCAI Facility- Primary site	To be provided to the Bidders on request The correspondence should clearly mention the Subject Line as indicated in the Title of the Tender Document
Address of RCAI Facility- Secondary site	To be provided to the Bidders on request The correspondence should clearly mention the Subject Line as indicated in the Title of the Tender Document

Name and Address where queries/correspondence concerning this Tender is to be sent	Office of CEO, National Internet Exchange of India9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001
	The correspondence should clearly mention the Subject Line as indicated in the Title of the Tender Document
Address where Bidders must submit Bid at the	**Office of CEO,** National Internet Exchange of India 9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001 The correspondence should clearly mention the Subject Line as indicated in the Title of the Tender Document
Evaluation method	QCBS (Quality and Cost Based Selection) method

Disclaimer

All the terms and conditions have been incorporated by NIXI after approval of the Competent Authority in NIXI. Any clause incorporated by the NIXI such as demanding Proof of Concept etc, incorporating any clause against the NIXI's policy and Preference to make in India Policy, mandating any Brand names or Foreign Certification, changing the default time period for Acceptance of material or payment timeline governed by OM of Department of Expenditure shall be null and void and would not be considered part of bid.

Further any reference of conditions published on any external site or reference to external documents / clauses shall also be null and void. If any seller has any objection / grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window being provided in the Prebid meeting and their pre-bid queries would be addressed/responded accordingly.

This Bid is also governed by the General Terms and Conditions.

While participating in bid, Bidder has to undertake compliance of the bid terms and conditions as laid in the RFP and any false declaration and non- compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

Table of Contents

Section I: Notice Inviting Tender (NIT)

1. Notice Inviting Tender (hereinafter referred to as “NIT”)

The Government of India enacted the Information Technology Act, 2000 for providing legal recognition to transactions carried out through electronic communications for e-Governance & eCommerce. CCA & NIXI have been jointly engaged under the Ministry of Electronics and Information Technology (MeitY) with the objective of promoting trust services in the electronic environment.

NIXI has come up with a detailed RFP towards Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers. NIXI intends to call for proposals from the eligible bidders who meet eligibility criteria set as indicated in the tender document, for setting up CCA Root Setup for SSL and setting up of CA set up for SSL including WebTrust Certification and incorporation of CCA root for SSL in Major Web Browsers.

2. The Tender

2.1. Bidders must go through the complete Tender Document for details before submission of their Bids.

2.2. Availability of the Tender Document: -The Tender Document shall be published on the NIXI Website. It shall be available for download after the date and time of the start of availability till the deadline for availability as mentioned on NIXI Portal.

2.3. **Clarifications:** - A Prospective Bidder requiring any clarification regarding the Tender Document may do so using NIXI Portal and may contact CEO, NIXI. Also, please feel free to contact Shri Rajiv Kumar Manager, (011- 48202000/02, Email: rajiv@nixi.in) NIXI for any query related to tender.

3. Eligibility Criteria for Participation in this Tender:

Subject to provisions in the Tender Document, participation in this Tender Process is limited to all bidders who fulfill the ‘Eligibility’ and ‘Qualification criteria as per the Tender Document.

1. The Bidder must: be a Company registered in India under the Indian Companies Act 1956/2013 as amended with their registered office in India for the last three years as on 31.03.2022.

2. The Bidder shall have revenue of INR 75 crores and shall be profitable for the last 3 financial years (FY 2021-22, 20-21, 19-20). The evidences shall be provided.

3. The bidder must:

   (i) not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of aforesaid reasons.

      a. Not stand declared ineligible/ suspended/ blacklisted/ banned/ debarred by Government from participation in its Tender Processes; and/ or

      b. Not be convicted (within three years preceding the last date of bid submission) or stand declared ineligible/ suspended/ blacklisted/ banned/ debarred by appropriate agencies of Government from participation in Tender Processes of all of its entities, for:

         i. offences involving moral turpitude in business dealings under the Prevention of Corruption Act, 1988 or any other law; and/or
         ii. offences under the Indian Penal Code or any other law for causing any loss of life/ limbs/ property or endangering Public Health during the execution of a public procurement contract and/ or
         iii. suspected to be or of doubtful loyalty to the Country or a National Security risk as determined by appropriate agencies of the Government of India.

      c. Not have changed its name or created a new “Allied Firm”, consequent to having declared ineligible/ suspended/ blacklisted/ banned/ debarred as above.

   (ii) Not have a conflict of interest, which substantially affects fair competition. The prices quoted should be competitive and without adopting any unfair/ unethical/ anti-competitive means. No attempt should be made to induce any other bidder to submit or not to submit an offer for restricting competition. To determine whether there has been an occurrence of act of conflict of interest, the decision by the Competent Authority of NIXI shall be final and binding.

4. The Bidder shall select the OEM with appropriate knowledge, experience and expertise in setting up, managing the Root and CA infrastructure and have expertise in handling WebTrust accreditation program and incorporation of CCA root for SSL in Major Web Browsers.

5. The Bidder shall engage the WebTrust Auditor, develop the complete design architecture, all required processes and complete the periodical audits of the infrastructure and perform the WebTrust certification program including incorporation of CA root in Major Web Browsers

6. The Bidder must also fulfill other additional eligibility condition(s), if any, as prescribed in Tender Document (including addendums; if issued).

Eligibility criteria for OEM (PKI Software):

Only PKI OEM who receive minimum overall 75% in the eligibility criteria for OEM will be shortlisted technically and deemed qualified for commercial evaluation.

Serial No	Eligibility Criteria	Category	Score	Supporting documentation
1*	Certificate Authority software quoted must be common criteria EAL 4+ or above certified along with support for Key profiles with both PKCS#11 and PKCS#12 support.	Mandatory	40	Copy of the certificate to be submitted
2*	OCSP Responder being quoted should be from the same OEM as that of CA Software provider to make it 100% compatible with the CA Software.	Mandatory	20	Copy of the OEM Authorization letter to be furnished.
3*	A single OEM should be a manufacturer of all the below components quoted: • Certificate Authority, • Registration Authority should be from a single OEM	Mandatory	20	Declaration from the OEM in the prescribed format signed by Authorized Signatory
4	The OEM should have local support & development center in India.	Mandatory	20	Declaration letter from the OEM mentioning address in the prescribed format signed by Authorized Signatory along with Certificate of Incorporation
5	The OEM shall have experience in establishing at least one WebTrust Accredited CA.	Mandatory	30	Certificate to the effect should be attached with the Technical Bid.
6	Certificate Authority and OCSP solution being quoted should have been implemented successfully and running for 3 years in at least one (01) Certifying Authorities.	Mandatory	20	Customer references letter in the prescribed format
7	OEM should have supplied & successfully implemented Certificate Authority and OCSP solution during the last 03 (Three) years till 31st March 2022 in at least 1 Root CA's	Mandatory	10	Customer references letter in the prescribed format
8	OEM should be actively participating in international policy making bodies/ committees like CAB Forum, WebTrust, IETF etc.	Mandatory	10	Declaration from the OEM mentioning the participation signed Authorized Signatory
9	Availability of Local Support in the same city	Mandatory	10	Declaration from the OEM mentioning local representative names and address.

Note: The points marked * are essential for qualifying and bidder must meet these points**.**

4. Purchase Preference Policies of the Government

As detailed in the Tender Document, NIXI reserves its right to grant preferences to eligible Bidders under various Government Policies/ directives (policies relating to Make in India (MII); MSME; Start-ups etc.).

5. Pre-bid Meeting:

Prospective Bidders may attend the Pre-bid Meeting (Offline/Online) for seeking clarification on Tender Document at the time, date, and place as mentioned in the Document and as per Notice in NIXI Portal (HTTPS://NIXI.IN)

Participation in such a Pre-bid Conference is not mandatory. If the prospective bidder does not participate or submit any query, then no subsequent representations from them with regard to Tender Document shall be entertained.

6. Submission of Bids:

Bids must be submitted by the Bidder in the Office of CEO, National Internet Exchange of India (NIXI), 9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001 till the deadline for submission mentioned in the Tender Document. **The Bidder will submit a Declaration to the Effect that no change of the Original Document has been made and they Comply with all the Terms and Conditions as per the Tender.**

Bidder must submit the bid complete in all respect; in the absence of which bid may be rejected.

7. Bid Opening

Bids received shall be opened at the specified date and time mentioned in the Tender Document.

8. Disclaimers and Rights of NIXI

The issue of the Tender Document does not imply that the NIXI is bound to select bid(s), and it reserves the right, without assigning any reason, to:

a) reject any or all of the Bids, or

b) cancel the tender process at any stage; or abandon the procurement of Equipment(s) and Services; or

c) issue another tender for identical or similar Equipment(s) and Services

SD/-

CEO, NIXI
National Internet Exchange of India (NIXI) 9th Floor, B-Wing,
Statesman House, 148, Barakhamba Road, New Delhi 110001

Section II: Instructions to Bidders (ITB)

1. The Tender Document

1.1 Basic Tender Details

The 'Tender Document' (hereinafter referred to as the 'the Tender Document') details the terms and conditions for entering into a contract for the execution of turnkey project (including design, supply, installation, testing, commissioning, training and acceptance of Equipment(s) and provisioning of Services as detailed in Section IV: "Bill of Material" (hereinafter referred to as 'BoM'). Bidders must go through the entire Tender Document for further details. In this Tender Document, any generic reference to 'Equipment' shall be deemed to include such Equipment(s) or Services or both.

1.2 Interpretations, Definitions, Abbreviations

Section III: General Conditions of Contract (GCC), detailed Tenets of interpretation (GCC-clause 1.1), Definitions (GCC-clause 1.2), and Abbreviations (GCC-clause 1.3), which shall also apply to the rest of the Tender Document.

1.3 Overview of Contents

1) The Sections, Forms and Formats comprising this Tender Document are described in Instructions to Bidders (ITB)-clauses 1.4, 1.5 and 1.6 below. Any generic reference to Tender Document shall also imply a reference to any/ all the sections, Forms, Formats and the BOM file or other files that comprise this Tender Document.

2) Bidder must submit the bid in the Forms/ Formats mentioned in ITB-clauses 1.5 and 1.6 below along with signed tender document along with its all corrigendum and addendums. Bidder must declare in his bid Form (Form 1) that it has read, understood, complied, and stands bound by all requirements.

1.4 Sections of the Tender Document

1.4.1 Sections of the Tender Document

The Tender Document contains the following sections, which are described in subsequent sub-clauses:

1) Section I: Notice Inviting Tender (NIT)

2) Section II: Instructions to Bidders (ITB)

3) Section III: General Conditions of Contract (GCC)

4) Section IV: Bill of Material (BoM)

5) Section V: Technical Specifications

6) Section VI: Qualification Criteria

1.4.2 Section I: Notice Inviting Tender (NIT)

Section I – Notice Inviting Tender (NIT) provides a synopsis of information relevant for a Bidder.

1.4.3 Section II: Instructions to Bidders (ITB)

Section II: "Instructions to Bidders" - ITB provides the relevant information as well as instructions to assist the prospective Bidders in preparation and submission of Bids. It also includes the mode and procedure adopted for receipt/ opening, scrutiny/ evaluation of Bids, and contract award.

1.4.4 Section III: General Conditions of Contract (GCC)

Section III – General Conditions of Contract (GCC) describe the conditions that shall govern the resulting contract. In case of any conflict, provisions of GCC shall prevail over those in ITB and in case of any conflict of this tender document from NIXI GTC, provisions of this tender document shall prevail over those in NIXI GTC.

1.4.5 Section IV: Bill of Material

Section IV – Bill of Material (BoM) describes the Equipment and Services required; Quantities and Units; City of Delivery; Bidder must fill-up 'Form 2: 'Bill of Material- Compliance'.

1.4.6 Section V – Technical Specifications

Section V – This Section lays down the technical specification of the Equipment and services required. Bidders must give Compliance for all the specifications in Form 3: Technical Specifications compliance.

1.4.7 Section VI: Qualification Criteria

Section VI: Qualification Criteria lay down the Qualifying Criteria for a bid/ Bidder to be considered a responsive bid/ bidder for further evaluation. Bids/ bidders not meeting these Qualification criteria shall be rejected as nonresponsive. Bidders must fill up 'Form 4: Confirmation for Qualification Criteria' and 'Form 4.1: Experience Statement'. Bidders shall attach statements and documents to confirm conformity to Qualification Criteria.

1.5 Forms (To be filled, digitally signed, and submitted by Bidders)

Please refer to clause 1.4 above to relate the following forms to the corresponding Sections.

1) Form 1: bid Form (To serve as a covering letter to both the Technical and Financial Bids)
    a) Form1.1: Bidder Information
    b) Form 1.2: Eligibility Declarations
    c) Form1.3: OEM's Authorization
2) Form 2: Bill of Material Compliance
3) Form 3: Technical Specifications- Compliance
4) Form 4: Qualification Criteria - Compliance

    (a) Form 4.1: Experience Statement
5) Form 5: Terms & Condition compliance
6) Form 6: Checklist for the Bidders
7) Form 7: Documents Relating to Bid Security

8) Form 8: Integrity Pact

9) Form 9: Make in India Certificate

Technical bid – BOM Sheet (**Only Unpriced Financial Sheet i.e. BOM** should be enclosed as part of the technical bid).

Signed tender document along with its all corrigendum and addendums should be enclosed as part of the technical bid.

1.6 Other Formats

1) Format1.1: Bank Guarantee Format for Performance Security

2) Format 1.2: No Claim Certificate

3) Format 2: Authorization for Attending Pre-bid Conference.

4) Form 10: Non-Disclosure Agreement (To be submitted by successful bidder/Contractor only)

2 NIXI - Rights and Disclaimers

2.1 NIXI

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. Root Certificate Authority Set up for SSL would also be established as part of the Tender.

The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The Office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures.

The Controller of Certifying Authorities (CCA) has established the Root Certifying Authority (RCAI) of India under section 18(b) of the IT Act to digitally sign the public keys of Certifying Authorities (CA) in the country. The RCAI is operated as per the standards laid down under the Act.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose, it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country. CCA in partnership with NIXI wants to take India forward in the direction of SSL certifications for the websites in addition to the present activities being handled by NIXI. NIXI’s present activities are as under:

NIXI is a not-for-profit Organization under section 8 of the Companies Act 2013, and was registered on 19th June, 2003. NIXI was set up for peering of ISPs among themselves for the purpose of routing the domestic traffic within the country, instead of taking it all the way to US/Abroad, thereby resulting in better quality of service (reduced latency) and reduced bandwidth charges for ISPs by saving on International Bandwidth. NIXI is managed and operated on a Neutral basis, in line with the best practices for such initiatives globally.

.IN is India's Country Code Top Level domain (ccTLD). The Govt. of India delegated the operations of IN Registry to NIXI in 2004. The IN Registry operates and manages India's .IN ccTLD.

Indian Registry for Internet Names and Numbers (IRINN) in India that provides allocation and registration services of IP addresses and AS numbers, and contributes to the society by providing Internet-related information as a non-profit, affiliation-based organization, and performing research, education and enlightenment activities. Through this Tender, NIXI wishes to establish SSL CA Setup and getting WebTrust Certification Done along with putting CCA's Root in major Web Browsers along with set up RCAI setup for CCA in DC and DR Sites.

Bids are to be addressed to

CEO, National Internet Exchange of India (NIXI)
9th Floor, B-Wing, Statesman House, 148,
Barakhamba Road, New Delhi 110001

The Tender Inviting Authority or its representative is the designated officer for submitting and clarifying about this Tender Document. NIXI may designate, as required, Officer and Consignee(s) and paying authority who shall discharge designated function during contract execution.

2.2 Right to Intellectual Property:

The Tender Document and associated correspondence shall always remain the property of the NIXI.

2.3 Right to Reject any or all Bids

The NIXI reserves its right to accept or reject any or all Bids, abandon/ cancel the Tender process at any stage, and issue another tender for the same or similar Equipment at any time before the award of the contract. It would incur no liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for such action(s).

2.4 Disclaimers

2.4.1 Regarding Purpose of the Tender Document

The Tender Document is neither an agreement nor an offer to prospective Bidder(s) or any other party hereunder. The purpose of the Tender Document is to provide the Bidder(s) with information to assist them in participation in this Tender Process.

2.4.2 Regarding Documents/ guidelines

The Tender Document, ensuing communications, and Contracts shall determine the legal and commercial relationship between the bidders/ contractors and the NIXI.

2.4.3 Regarding Information Provided

Information contained in the Tender Document or subsequently provided to the Bidder(s) is on the terms and conditions set out in the Tender Document or subject to which that was provided. Similar terms apply to information provided in documentary or any other form, directly or indirectly, by the NIXI or any of its authorized employees or its associated agencies.

2.4.4 Regarding Tender Document:

a) The Tender Document does not purport to contain all the information Bidder(s) may require. It may not address the needs of all Bidders. They should conduct due diligence, and analysis, check the information's accuracy, reliability, and completeness, and may obtain independent advice from appropriate sources. Information provided in the Tender Document to the Bidder(s) is on a wide range of matters, some of which may depend upon interpreting the law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The NIXI, its employees and other associated agencies accept no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

b) The NIXI, its employees and other associated agencies make no representation or warranty for the accuracy, adequacy, correctness, completeness or reliability, assessment, assumption, statement, or information in the Tender Document. They have no legal liability, whether resulting from negligence or otherwise, for any loss, damages, cost, or expense that may arise from/ incurred/ suffered howsoever caused to any person, including any Bidder, on such account.

3 Bidders - Eligibility and Preferential Policies

3.1 Bidders

Subject to provisions in the following clauses in this section and provisions in Tender Document, this invitation for Bids is open to all bidders who fulfill the ‘Eligibility Criteria’ and ‘Qualification Criteria’ stipulated in the Tender Document.

4 Purchase Preference Policies of the Government

NIXI reserves its right to grant preferences to the following categories of eligible Bidders under various Government Policies/ Directives:

a) Class I Local Suppliers under Public Procurement [Preference to Make in India (MII)] Order 2017” of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised from time to time.

b) Bidders from Micro and/ or Small Enterprises (MSEs) under Public Procurement Policy for the Micro and Small Enterprises (MSEs) Order, 2012 as amended from time to time.

c) Start-ups Bidders under Ministry of Finance, Department of Expenditure, Public Procurement Division OM No F.20/212014-PPD dated 25.07.2016 and subsequent clarifications.

4.1 Purchase Preference to Make in India

Purchase preference to make in India would be provided in line with the Letter no. P-45021/2/2017-PP (BE-II). Dated 16th September, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI as amended from time to time.

4.1.1 Definition of Local Content and Categories of Local Suppliers

Bidders/Contractors are divided into three categories based on Local Content. Local content in the context of this policy is the total value of the equipment(s) procured (excluding net domestic indirect taxes) minus the value of imported content in the equipment(s) (including all customs duties) as a proportion of the total value, in percent.

a) 'Class-I local Supplier' is a supplier with local content equal to or more than 50%.
b) 'Class-II local Supplier' is a supplier with local content equal to or more than 20%, but less than that applicable for Class-I local Supplier.
c) 'Non - Local Supplier' is a supplier with local content less than that applicable for Class-II local Supplier, in sub-clause above.
d) The margin of purchase preference shall be 20%.

4.1.2 Eligibility to participate

a) Classes of Local Suppliers eligible to Participate: Based on the Make in India Policy, only Class-I and Class-II local Suppliers shall be eligible to participate in this bid.
b) Minimum local content for eligibility to participate shall be 20%.
c) Non- local suppliers are not eligible to participate in this bid.

4.1.3 Classification of Procurement and Purchase Preference Methodology (Two Bid Process):

The Bidders will submit their technical bid in sealed envelope and the Commercial Bid in separate Envelope and both the Technical and Commercial Bids will be put together in a bigger envelope and then the bigger envelope will be sealed. The bigger envelope should have address of CEO, National Internet Exchange of India (NIXI), 9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001. It should clearly mention that it a bid for “Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers.”

In the first phase, the Technical bids will be opened and evaluated based on the experience and expertise in setting up the infrastructure and conducting WebTrust Audit along with incorporation of SSL Root in major web browsers and the Commercial Bids of the successful technical Bidders will be opened and Commercial Bids will be evaluated and the L1 bidder will be evaluated as per the criteria as mentioned (as per Bill of Materials, and as per Format for Commercial Bids) in the tender documents.

4.1.4 Verification of local content and violations:

1) The 'Class-I local Supplier'/ 'Class-II local Supplier' at the time of tender, bidding, or solicitation shall be required to indicate the percentage of local content and provide self-certification that the equipment(s) offered meets the local content requirement for 'Class-I local Supplier'/ 'Class-II local Supplier', as the case may be.

2) The 'Class-I local Supplier'/ 'Class-II local Supplier' shall be required to provide a certificate

from the statutory auditor or cost auditor of the company (in the case of companies) giving the percentage of local content as specified in Form- 9.

3) Bids with false declarations regarding Local contents shall be rejected as non- responsive, in addition to punitive actions under the MII orders.

4.1.5 Support to Start-ups

Relaxation in Prior Turnover: Relaxation in the prior turnover for start-up enterprises (subject to meeting of quality & technical specifications) has been provided. However, Start-ups must fulfill the prior experience Criteria as defined under Section-VI – Qualification Criteria.

5 Bid Prices, Taxes and Duties

5.1 Prices

5.1.1 Competitive and Independent Prices

a) The prices should be arrived at independently, without restricting competition, any consultation, communication, or agreement with any other bidder or competitor relating to:

   i) those prices; or
   ii) the intention to submit an offer; or
   iii) the methods or factors used to calculate the prices offered.

b) The prices should neither be nor shall be knowingly disclosed by the Bidder, directly or indirectly, to any other bidder or competitor before bid opening or contract award unless otherwise required by law.

5.1.2 Price Schedule

1) Bidders are to quote value of each line item in Financial Bid (BOM) as per the Tender Document. In case of any discrepancy between rates mentioned in figures and words, the later shall prevail. In case of any arithmetic mistake committed by bidder in financial bid (BOM) then NIXI reserve the right to correct the same by taking unit price quoted by the bidder and quantities specified by the NIXI.

2) Bidders shall fill in their rates other than zero value. Bid will be liable to be rejected if bidder has filled Rs. 0 (zero) for any line item.

3) The quoted unit price shall be considered to include all relevant financial implications.

5.1.3 Currencies of Bid and Payment

The currency of bid and payment shall only be Indian Rupees. All payments shall also be made in Indian Rupees only.

5.1.4 Non-compliance

Tenders, where prices are quoted in any other way, may be rejected as non-responsive.

5.2 Firm/ Variable Price

5.2.1 Firm Price

Prices quoted by Bidder shall remain firm and fixed during the currency of the contract and no variation on higher side on any account.

5.3 Goods and Services Tax (GST)

1) Bidders should ensure that they are GST compliant Bidder should be registered under GST and furnish GSTIN number and GST Registration Certificate in their bids.
2) Bidder/Contractor undertakes that in case of non-compliance by the Bidder(s) of the GST provisions which results in blockage/reversal of any input tax credit to NIXI, Bidder/Contractor shall be liable to indemnify the NIXI any such loss of input credit including interest, penalty and all incidental expenses incurred by NIXI. Such indemnification may also be by way of invocation of any security deposit, deduction from any payment that NIXI has to make to the Bidder/ Contractor, as per the discretion of the NIXI.
3) Bidder/Contractor undertakes to raise invoice within 10 days from date when the right to raise invoice and demand for payment accrues as per the contract terms. In case invoice is raised and submitted before the due date; then NIXI reserves the right to return such invoice(s) to the Bidder/Contractor. In such a situation Bidder/Contractor would be required to raise fresh invoice as per the contract terms.
4) If the Bidder/Contractor fails to adhere the terms & conditions of the contract and NIXI will deduct Liquidated Damages and/or SLA penalties for the same, then in such a case; NIXI will charge GST over and above the Liquidated Damages and/or SLA penalties; as the case may be; and same shall be recovered from the Bidder/Contractor. This may vary; depending on the position of law on the date when such deduction is made.
5) Along with the invoice; Bidder/Contractor would be required to submit relevant documentary evidence to the effect that invoice submitted was issued either through e- Invoice system of GST or has been updated on GSTN portal using Invoice Furnishing Facility (IFF).
6) In case, in future any GST liability is required to be borne by NIXI; which was the responsibility of the Bidder/Contractor, then the same shall be claimed from the Bidder/Contractor by way of raising debit notes.
7) NIXI reserves the right to ask the Bidder/Contractor to submit relevant documents to ensure that they are GST compliant and in such a case Bidder/Contractor shall forthwith provide all such documents as may be required by NIXI.

5.4 Payments

5.4.1 General

Payment terms laid down in clause GCC 10 shall be applicable.

5.4.2 No Advance Payments

No advance payment of any type (Mobilization, secured advances etc.), shall be made by the NIXI to the contractor.

6 Downloading the Tender Document; Corrigenda and Clarifications

6.1 Downloading the Tender Document

The Tender Document shall be published and be available for download as mentioned on NIXI Website Portal. The Bidders can obtain the Tender Document after the date and time of the start of availability till the deadline for availability. If the office happens to be closed on the deadline for the availability of the Tender Document, the deadline shall not be extended.

6.2 Corrigenda/ Addenda to Tender Document

Before the deadline for submitting bids, the NIXI may update, amend, modify, or supplement the information, assessment or assumptions contained in the Tender Document by issuing corrigenda and addenda. The corrigenda and addenda shall be published in the same manner as the original Tender Document (i.e. NIXI Website). Without any liability or obligation, the Portal may send intimation of such corrigenda/ addenda to bidders who have downloaded the document under their login. However, the bidders' responsibility is to check the NIXI Website for any corrigenda/ addenda. Any corrigendum or addendum thus issued shall be considered a part of the Tender Document. To give reasonable time to the prospective bidders to take such corrigendum/ addendum into account in preparing their bids, the NIXI may suitably extend the deadline for the bid submission, as necessary. After the NIXI makes such modifications, any Bidder who has submitted his bid in response to the original invitation shall have the opportunity to either withdraw his bid or re-submit his bid superseding the original bid within the extended time of submission.

6.3 Clarification on the Tender Document

A Bidder may seek clarification of the Tender Document through written Communications in the name of CEO, NIXI in the given address, **provided the clarifications are raised one day before the Pre-Bid meeting**. The response to the clarifications (If any) shall be shared on the NIXI Portal. Any modification of the Tender Document that may become necessary in view of response given to the clarification; shall be made by the NIXI by issuing an Addendum/ Corrigendum as per the sub-clause 6.2 above.

7 Pre-bid Meeting

1) Prospective bidders interested in participating in this tender may attend a Pre- bid Meeting (Offline/Online/Hybrid Mode) (at venue, date and time specified above) to seek clarification to the Tender Document.

2) Participation is not mandatory. However, if a bidder chooses not to (or fails to) participate in the Pre-bid conference and/or does not submit a written query to NIXI before the Pre-Bid Meeting, it shall be assumed that they have participated in this tender process only after understanding the tender document in its entirety.

3) Delegates participating in the Pre-bid Meeting must provide a photo identity and an authorization letter as per the format in Format 2: "Authorization for attending a Pre-bid Conference" from their organization; else, they may not be allowed to participate. The pre-bid Meeting may also be held online or offline mode at the discretion of the NIXI. Maximum of two People from an organization will be allowed to attend the Pre-bid Meeting.

4) After the Pre-bid Meeting, clarifications (if required) shall be published on the NIXI’s website(https://NIXI.gov.in). If required, a corrigendum to the Tender Document shall be

issued, containing amendments to the provision(s) of the Tender Document, which shall form integral part of the Tender Document. To give reasonable time to the prospective bidders to take such clarifications into account in preparing their bids, the NIXI may suitably extend, as necessary, the deadline for the bid submission.

8 Preparation of Bids

8.1 The bid

8.1.1 Language of the bid

The bid submitted by Bidder and all subsequent correspondence and documents relating to the bid exchanged between Bidder and the NIXI shall be written in English. However, the language of any printed literature furnished by Bidder in connection with its bid may be written in any other language provided a translation accompanies the same in the bid language. For purposes of interpretation of the bid, translation in the language of the bid shall prevail.

8.1.2 Local Conditions and Factors

Bidders shall themselves be responsible for compliance with Rules, Regulations, Laws and Acts in force from time to time at relevant places. On such matters, the NIXI shall have no responsibility and shall not entertain any request from the bidders in these regards.

8.1.3 Cost of Bidding

The Bidder(s) shall bear all direct or consequential costs, losses and expenditure associated with or relating to the preparation, submission, and subsequent processing of their Bids, including but not limited to preparation, copying, postage, submitting, downloading, delivery fees, expenses associated with any submission of samples, demonstrations, or presentations which the NIXI may require, or any other costs incurred in connection with or relating to their Bids. All such costs, losses and expenses shall remain with the Bidder(s), and the NIXI shall not be liable in any manner whatsoever for the same or any other costs, losses and expenses incurred by a Bidder(s) for participation in the Tender Process, regardless of the conduct or outcome of the Tender Process.

8.1.4 Interpretation of Provisions of the Tender Document

The provisions in the Tender Document must be interpreted in the context in which these appear. Any interpretation of these provisions for remote from such context or other contrived or in between-the-lines interpretation is unacceptable.

8.1.5 Alternative Bids not allowed

Conditional offers, alternative offers, multiple bids by a bidder shall not be considered.

8.1.6 Technical bid

"Technical Bid" shall include inter-alia the original or scanned copies of duly inked signed or digitally signed copies of the following documents in .pdf format. Pdf documents should not be password protected. ***No price details should be given or hinted in the Technical bid, in case the bidder provides any price details in technical bid, their bid shall be liable to rejected.***

1) Form 7: Documents relating to Bid Security: A Bid Securing Declaration (BSD) in lieu of bid security in the format provided therein shall submitted in the Technical Bid.

2) Form 1: bid Form (to serve as covering letter and declarations applicable for both the Technical bid and Financial bid);

   a) Form 1.1: Bidder Information;
   b) Form 1.2: Eligibility Declarations;
   c) Form 1.3: OEM's Authorization: Bidder must have been duly authorized by the eligible OEMs to quote for and supply the Equipment to the NIXI in this particular tender specifically. Bidder shall submit OEM's authorization letter to this effect as per this. Also, the OEM should declare that the equipment is not end of Sale before Installation and End of Support for next 5 years. OEM will declare that they will support the equipment for at least next 5 Years from original date of Installation and Commissioning. OEM Shall declare these in the Letter Head.

      OEM (software, hardware) undertaking stating OEM's support to CCA/NIXI in case of the termination of contract with bidder.

   d) NIXI reserves the right to en-cash the PBG (Performance Bank Guarantee) and Bid Guarantee submitted by the Bidder in case the Bidder fails to carry out the Installation Commissioning, to get WebTrust certification and incorporation of CCA roots in Major Web Browsers in the stipulated time (1 year from the date of Contract/PO).

3) Form 4: 'Qualification Criteria- Compliance': Documentary evidence needed to establish the Bidder's qualifications as stipulated in Section VI: Qualification Criteria as follows.

   Besides the stipulated documents, other supporting documents, literature, pamphlets may also be attached.

   - Bidder shall also submit Form 4.1: Experience Statement to prove its technical, production and financial capabilities and eligibility, commensurate with requirements of this Tender.

4) Form 2: Bill of Material (BoM) - Compliance: Bidders should fill this form as a compliance of Equipment & Services offered by them, maintaining the same numbering and structure. Bidder shall also provide compliance statement of Schedule-IV as per attached Form 2.

5) Form 3 - Technical Specifications- Compliance: Bidder shall submit the required and relevant documents like complete design architecture for DC and DR sites, technical data, literature, drawings, datasheets, test Reports/ Certificates and or/ or Type Test Certificates (if applicable/ necessary) with supporting documents, to establish that the Equipment and Services offered in the bid fully conform to the Equipment and Services specified by the NIXI in the Tender Document. Bidder shall also provide compliance statement of Schedule-V along with Form 3.

6) Form 5 – Terms and Condition - Compliance: Bidder must submit compliance

of Terms & conditions as per Form-5 Form

7) Form 6- Checklist for the Bidders. Bidder must also submit the Checklist given in the Tender Document as Form 6 to confirm that it has complied with all the instructions in the Tender Document, and nothing is inadvertently left out. This checklist is only for general guidance and is not comprehensive, and does not absolve Bidder from complying with all the requirements stipulated elsewhere in the Tender Document.

8) Duly signed Form 8: Integrity Pact.

9) Form 9 : Make in India Certificate [To be certified by statutory auditor or cost auditor of the company (in the case of companies) for a tender value above Rs. 10 crores giving the percentage of local content].

8.1.7 Financial bid

"Financial bid" shall comprise the Price Schedule considering all financially relevant details, including Taxes and Duties as per Financial Bid (BOM) Proforma.

8.2 Bid Validity

1) Bid Life Cycle (From Publish Date): 90 Days

2) Bid Offer Validity (From End Date): 75 Days

3) A bid valid for a shorter period shall be rejected as nonresponsive.

4) If required, before the expiry of the original time limit, the NIXI may request the bidders to extend the validity period for a specified additional period. The request and the bidders' responses shall be made in writing or electronically. A bidder may agree to or reject the request. A bidder who has agreed to the NIXI's request for extension of bid validity, in no case, he shall be permitted to modify his bid.

8.3 Bid Security - Related Documents

1) All Bidders shall furnish/ submit a Bid Securing Declaration (BSD) as Form 7: Documents Relating to Bid Security, along with its Technical bid. The BSD is required to protect the NIXI against the risk of the Bidder's unwarranted conduct as amplified under the sub-clause below.

2) The BSD provides for automatic suspension of the Bidder from being eligible for bidding in any tender in NIXI for 2 years from the date of such enforcement. This declaration shall stand enforced if Bidder breaches the following obligation(s) under the tender conditions:

   (a) withdraws or amends his bid or impairs or derogates from the bid in any respect within the period of validity of its bid; or

   (b) after having been notified within the period of bid validity of the acceptance of his bid by the NIXI:

refuses to or fails to submit the original documents for scrutiny and/or the required Performance Security within the stipulated time as per the conditions of the Tender Document.

3) Unsuccessful Bidders' bid-securing declaration shall expire, if the contract is not awarded to them, upon:

   a) receipt by Bidder of the NIXI's notification of cancellation of the entire tender process or rejection of all bids or
   b) of the name of the successful bidder or
   c) forty-five days after the expiration of the bid validity (including any extension thereof)

4) The bid-Securing Declaration of the successful bidder shall stand expired only when Bidder has furnished the required Performance Security.

8.4 Non-compliance with these provisions

Bids are liable to be rejected as nonresponsive if a Bidder:

1) fails to provide and/ or comply with the required information, instructions etc., incorporated in the Tender Document or gives evasive information/ reply against any such stipulations.

2) furnishes wrong and/ or misguiding data, statement(s) etc. In such a situation, besides rejection of the bid as nonresponsive, NIXI will enforce Bid Security Declaration in such cases.

9 Signing and Submitting of Bids

9.1 Relationship between Bidder and e Procurement Portal (NIXI Portal)

NIXI will be floating the tender for Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers. Hence, NIXI's portal for Tender will be used and any changes including corrigendum etc. would be published in NIXI Portal Only.

9.2 Signing of bid

The individual signing the bid or any other connected documents should submit Copy of Board Resolution and/ or Power of attorney on Stamp Paper for authorized signatory, which authorizes the signatory to commit and submit bids on behalf of the bidder in Form 1.1: Bidder Information. In case the bidder is awarded the contract then the person authorized by the bidder shall continue to act as the authorized representative of the bidder till the time of completion of contract. Any change in authorized signatory be informed forthwith to NIXI along with the relevant document of authorized signatory.

9.3 Submission of Bids.

9.3.1 Submission/ Submitting at Site (as mentioned in the tender Document)

1) In the case of downloaded documents, Bidder must not make any changes to the contents of the documents while submitting, except for filling the required information – otherwise, the bid shall be rejected as nonresponsive. In case of any changes in the Tender documents, it will be presumed that the tender documents in original has not been changed and terms and conditions and other conditions are bidding on the Bidder.

   Bids shall be received only in the Office of CEO, NIXI, National Internet Exchange of India (NIXI) 9th Floor, B-Wing, Statesman House, 148, Barakhamba Road, New Delhi 110001.

2) on or before the deadline for the bid submission.

3) Only one copy of the bid can be submitted, and Bidder shall sign all statements, documents, certificates submitted by him, owning sole and complete responsibility for their correctness/ authenticity as per the provisions of the IT Act 2000 as amended from time to time.

4) Bidders need to sign and submit the Tender Document along with its corrigendum & amendments. It is assumed that Bidder commits itself to comply with all the Sections and documents submitted by the Tender Inviting Officer.

5) Bidder must submit scanned copies of originals (or self-attested copies of originals – as specified). Submitted pdf documents should not be password protected. Bidder should ensure the clarity/ legibility of the scanned documents submitted by him.

6) The NIXI reserves its right to call for verification originals of all such self- certified documents submitted by any of the bidders; at any stage of evaluation, especially from the successful Bidder(s) before the issue of Purchase Order.

7) **Bidder shall submit the price as per Financial Bid (BOM) in NIXI without any Zero values in the unit price column.**

8) The date and time of the deadline for the bid submission shall be the next working day if the specified date is declared a holiday for the Tender Inviting Office.

9) The NIXI shall not be responsible for any failure, malfunction or breakdown of the electronic system issues with Website at the last minutes during the Tender Process. Bidders are advised to Download the Tender Documents well in advance for submission of the bids

10) The NIXI may extend the deadline for bids submission in which case all rights and obligations of the NIXI and the bidders previously subject to the original deadline shall then be subject to the new deadline for the bid submission.

11) Bid submitted through modalities other than those stipulated in tender document shall be liable to be rejected as nonresponsive.

9.3.2 Implied acceptance of procedures by Bidders

Submission of bid in response to the Tender Document is deemed to be acceptance of the NIXI and tender procedures and terms & conditions of the Tender Document.

9.3.3 Withdrawal of Bids

1) The bidder may withdraw his bid before the bid submission deadline.
2) No bid should be withdrawn after the deadline for the bid submission and before the expiry of the bid validity period. If a Bidder withdraws the bid during this period, the NIXI shall be within its right to enforce Bid Securing Declaration in addition to other punitive actions provided in the Tender Document for such misdemeanor.

10 Bid Opening

The date & time of the opening bid is as stipulated in the Tender Document.

11 Evaluation of Bids and Award of Contract

11.1 General norms

11.1.1 Evaluation based only on declared criteria.

The evaluation shall be based upon scrutiny and examination of all relevant data and details submitted by Bidder in its bid and other allied information deemed appropriate by NIXI. Evaluation of bids shall be based only on the criteria/ conditions included in the Tender Document.

11.1.2 Minor Infirmity

1) In case of any minor infirmity in the bid document of bidder, the decision of the NIXI shall be final in this regard.

2) Wherever necessary; NIXI shall convey its observation to Bidder through NIXI asking Bidder to respond by a specified date. If Bidder does not reply by the specified date or gives an evasive reply without clarifying the point at issue in clear terms, that bid shall be liable to be rejected as non-responsive.

11.1.3 Clarification of Bids and shortfall documents

1) During the evaluation of Technical or Financial Bids, the NIXI may, at its discretion, but without any obligation to do so, ask Bidder to clarify its bid within 3 days. The request for clarification shall be notified on NIXI Portal, and no change in prices or substance of the bid shall be sought, offered, or permitted that may grant any undue advantage to such bidder.

2) NIXI may ask original documents of submitted scanned copies. If any substantive discrepancy found between original and scanned submitted copies; then the bid shall be liable to be rejected as non-responsive in NIXI may enforce Bid Security declaration.

3) The NIXI reserves its right to, but without any obligation to do so, to seek any shortfall information/ documents only in case of historical documents which pre- existed at the time of the tender opening, and which have not undergone change

since then. There is a provision on the portal for requesting Short-fall documents from the bidders. The system allows taking the shortfall documents from any bidders as per NIXI procedure after the technical bid opening.

11.1.4 Contacting NIXI during the evaluation

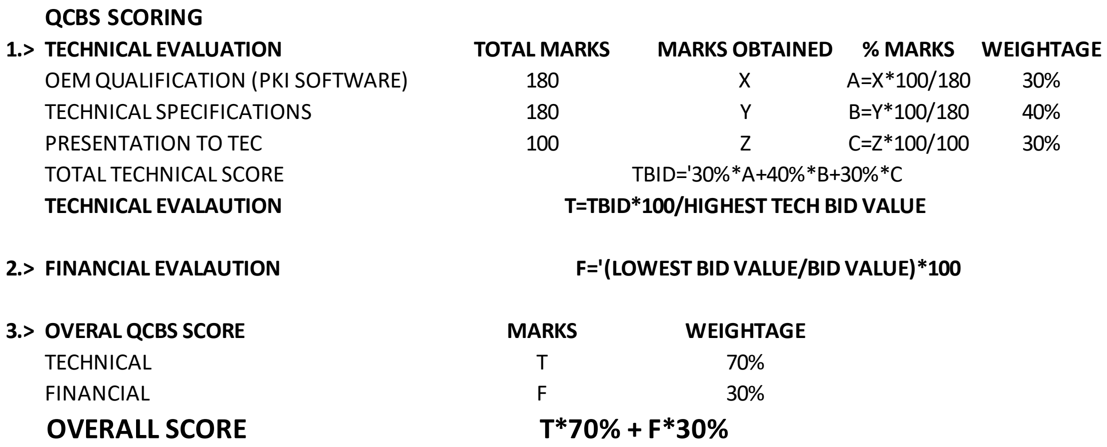
From the time of bid submission to awarding the contract, no Bidder shall contact the NIXI on any matter relating to the submitted bid. If a Bidder needs to contact the NIXI for any reason relating to this tender and/ or its bid, it should do so only in writing or electronically. Any effort by a Bidder to influence the NIXI during the processing of bids, evaluation, bid comparison or award decisions shall be construed as a violation and bid shall be liable to be rejected as nonresponsive in addition to enforcement of Bid Security declaration.

11.2 Evaluation of Bids

11.2.1 The evaluation process:

This Tender Process comprises of two Bid system i.e. Technical and Financial Bids. Initially, only the technical bids shall be opened on the stipulated date of opening of bids. After that, the technical bids evaluation shall be done to ascertain whether and how many bids are meeting the eligibility, qualification criteria and Technical aspects. Opening of financial bids and their evaluation will be done in respect of only those bids which were submitted by those Bidders whose technical bid are declared successful after the evaluation process.

The selection of the best evaluated bidder will be done by following QCBS (Quality and Cost Based Selection) method. The bids received will be given technical and financial scores. For final evaluation the technical scores will be given a weightage of 70% while the commercial score will be awarded a weightage of 30%. The bidder scoring the highest total weighted average score will be considered the most suitable bidder for the award of the contract. The scores shall be calculated as given in table below:



	QCBS SCORING				
1.>	**TECHNICAL EVALUATION**	**TOTAL MARKS**	**MARKS OBTAINED**	**% MARKS**	**WEIGHTAGE**
	OEM QUALIFICATION (PKI SOFTWARE)	180	X	A=X*100/180	30%
	TECHNICAL SPECIFICATIONS	180	Y	B=Y*100/180	40%
	PRESENTATION TO TEC	100	Z	C=Z*100/100	30%
	TOTAL TECHNICAL SCORE		TBID='30%*A+40%*B+30%*C		
	TECHNICAL EVALAUTION		**T=TBID*100/HIGHEST TECH BID VALUE**		
2.>	**FINANCIAL EVALAUTION**		**F='(LOWEST BID VALUE/BID VALUE)*100**		
3.>	**OVERAL QCBS SCORE**	**MARKS**	**WEIGHTAGE**		
	TECHNICAL	T	70%		
	FINANCIAL	F	30%		
	OVERALL SCORE	**T*70% + F*30%**			

ILLUSTRATION OF BID EVALAUTION:

A.> BIDDER 1:

TECHNICAL EVALUATION	TOTAL MARKS	MARKS OBTAINED	% MARKS	WEIGHTAGE	WEIGHTED SCORE
OEM QUALIFICATION (PKI SOFTWARE)	180	160	89	30%	**26.67**
TECHNICAL SPECIFICATIONS	180	140	78	40%	**31.11**
PRESENTATION TO TEC	100	80	80	30%	**24.00**
TOTAL TECHNICAL SCORE, TBID1					**81.78**
FINANCIAL BID VALUE (IN LAKHS),FBID1					**900**

B.> BIDDER 2:

TECHNICAL EVALUATION	TOTAL MARKS	MARKS OBTAINED	% MARKS	WEIGHTAGE	WEIGHTED SCORE
OEM QUALIFICATION (PKI SOFTWARE)	180	140	78	30%	**23.33**
TECHNICAL SPECIFICATIONS	180	100	56	40%	**22.22**
PRESENTATION TO TEC	100	90	90	30%	**27.00**
TOTAL TECHNICAL SCORE, TBID2					**72.56**
FINANCIAL BID VALUE (IN LAKHS),FBID2					**700**

C.> BIDDER 3:

TECHNICAL EVALUATION	TOTAL MARKS	MARKS OBTAINED	% MARKS	WEIGHTAGE	WEIGHTED SCORE
OEM QUALIFICATION (PKI SOFTWARE)	180	180	100	30%	**30.00**
TECHNICAL SPECIFICATIONS	180	180	100	40%	**40.00**
PRESENTATION TO TEC	100	90	90	30%	**27.00**
TOTAL TECHNICAL SCORE, TBID3					**97.00**
FINANCIAL BID VALUE (IN LAKHS),FBID3					**1200**

FINAL EVLAUTION OF THREE BIDS

TECHNICAL WEIGHTAGE FOR FINALISATION	**70%**		
FINANCIAL WEIGHTAGE FOR FINALIZATION	**30%**		

	TBID1	TBID2	TBID3
BID FINAL TECHNICAL SCORE	**81.78**	**72.56**	**97.00**
BID FINAL FINANCIALS (IN LAKHS)	**900**	**700**	**1200**

FINAL TECHNICAL WEIGHTED SCORE	**59.0**	**52.4**	**70.0**
FINAL FINANCIAL WEIGHTED SCORE	**23.3**	**30.0**	**17.5**
FINAL COMBINED SCORE FOR BIDDER	**82.3**	**82.4**	**87.5**

If NIXI considers necessary, revised financial bids may be called from eligible bidders before opening of financial bid.

11.3 Technical Evaluation

Only substantively responsive bids shall be evaluated for technical evaluation. In evaluating the technical bid, conformity to the eligibility and qualification criteria, technical specifications of the offered Equipment and Services in comparison to those specified in the Tender Document will be ascertained. Additional factors incorporated in the Tender Document shall also be considered in the manner indicated there-in. Bids with deviations shall be rejected as non- responsive. NIXI reserves its right to consider and allow minor infirmity in technical Conditions as per ITB-clause 11.1.2.

PKI OEM who receives overall 75% or more in the eligibility criteria for OEM and also qualify for all the points marked starred, will be shortlisted technically and deemed qualified for commercial evaluation.

Bidders who receive overall 75% or more in technical specification (in Section V) will be qualified. It is also informed that bidders must also score 75% in each section marked starred of the technical specification in Section V for technical evaluation.

The technical evaluation will be based upon following only for eligible and qualified bidders:

- 30% Weightage: %Marks in the eligibility criteria for OEM (Section I clause 3)
- 40% Weightage: %Marks in the Technical Specifications (Section V)
- 30% Weightage: %Marks for Presentation to TEC committee during Technical Evaluation.

For the Technical Evaluation of the bids, Bidder shall provide a detailed presentation to the Technical Evaluation Committee (TEC) covering complete system design, architecture, specifications of all equipments (hardware and software's),update on 100% compliance on the complete checklist as per Annexure, overall design objectives including performance parameters and business continuity, methodology and implementation plan including WebTrust and CAB certifications, profile of team, bidder knowledge and experience in establishing CA setups etc.

11.3.1 Evaluation of Eligibility

NIXI shall determine, to its satisfaction, whether the Bidders are eligible as per Tender Document to participate in the Tender Process as per submission in Form 1.2: Eligibility Declarations in Form 1: Bid Form. Bids that do not meet the required eligibility criteria prescribed shall be rejected as nonresponsive.

11.3.2 Evaluation of Qualification Criteria

NIXI shall determine, to its satisfaction, whether the Bidders are qualified and capable in all respects to perform the Contract satisfactorily (subject to relaxation, as per tender document, for MSME/Start-ups) as per submission in Form 4 and its Form 4.1. This determination shall, inter-alia, consider the Bidder's financial, technical or other prescribed eligibility for meeting requirements incorporated in the Tender Document.

11.3.3 Evaluation of Conformity to Bill of Material and Technical Specifications and other parameters specified in Tender document

Technical Evaluation Committee (TEC) will shortlist Technical Bids on the basis of technical solution, conformity of technical specifications, parameters, features offered vis- à-vis tendered specifications requirements, etc. The short-listed bidders shall be asked for a detailed technical presentation, discussion on the solution and items offered in the bid. Further, TEC may ask the bidder to bring any selected items, sub items of their quoted items for technical evaluation at NIXI or any other location decided by TEC in specified time limit within three days. In case, bidder fails to bring their quoted items within the stipulated time, for whatever reasons, their bid will not be considered for further evaluation. It is bidder's responsibility to showcase the desired parameter quoted in the bid by bidder. To do this, if bidder has to bring different tools, it will be responsibility of bidder to arrange at no cost to NIXI.

11.4 Evaluation of Financial Bids

11.4.1 Financial Bids

1) Evaluation of the financial bids shall be on the price criteria only. Financial Bids of all technically qualified bids will be evaluated and the financial weightage of the bidders will be determined as per the QCBS Procedure as mentioned above.

2) The comparison of the responsive Bids shall be on Total bid price of all the Equipment & Services quoted by the bidder in the price bid.

3) In line with the policies of the Government of India, as amended from time to time, NIXI reserves the right to give purchase preferences to eligible categories of Bidders as indicated in the Tender Document.

4) Bidder must submit Price Break up {(Financial Bid (BoM)} sheet during Bid submission price

12 Award of Contract

12.1 The NIXI's Rights

12.1.1 Right to Vary Quantities

During the Contract period, NIXI reserves the right to increase or decrease the quantity of Equipment originally stipulated in Section IV: Bill of Material, without any change in the unit prices or other terms and conditions of the bid and the Tender Document, provided this increase/ decrease shall not exceed 25 (twenty-five) percent of stipulated quantities. In case of increase of quantity, NIXI will give reasonable notice and sufficient delivery & commissioning period.

12.2 Signing of Non-Disclosure Agreement

1) The Successful Bidder/Contractor shall sign a Non-Disclosure Agreement (NDA) with NIXI as per Form-10 and submit the same within 14 days from the date of issue of contract.

2) The successful bidder shall also sign a Non-Disclosure Agreement with employees who are deployed in this project during implementation and operations.

3) The Successful Bidder/Contractor shall ensure that all persons, employees, workers and other individuals engaged by Bidder in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by the Bidder unless such person is found to be suitable in such verification and Bidder shall retain the records of such verification and shall produce the same to NIXI as and when requested. NIXI may also, if required, go for verification of manpower of contractor engaged for this project from government agencies.

12.3 Issuance of Contract

12.3.1 Selection of Successful Bidder

The NIXI shall award the contract to the Bidder whose bid is technically successful and scored highest 1 based on QCBS procedure, if its final price is found to be reasonable, as per evaluation criteria detailed in the Tender Document.

12.3.2 Performance Security

Within fourteen (14) days of issuance of contract by NIXI, performance Security as per details in GCC-5.7 shall be submitted by the successful bidder to the NIXI and if it fails to do so within the specified period, it shall be lawful for NIXI at its discretion to annul the award and enforce Bid Securing Declaration.

12.3.3 Right to Cancellation of the Tender Process:

NIXI reserves the right to cancel the Tender at any stage of the Tender Process without assigning any reasons whatsoever.

13 Integrity Pact:

The bidder must comply with the Integrity Pact (IP) as a preliminary qualification and sign the Integrity Pact (IP) as at Form 8.

Section III: General Conditions of Contract (GCC)

1. General

1.1 Tenets of Interpretation

Unless where the context requires otherwise, throughout the contract:

1) The heading of these conditions shall not affect the interpretation or construction thereof.
2) Writing or written includes matter either whole or in part, in digital communications, manuscript, typewritten, lithographed, cyclostyled, photographed, or printed under or over signature or seal or digitally acceptable authentication, as the case may be.
3) Words in the singular include the plural and vice-versa.
4) Words importing the masculine gender shall be taken to include other genders, and words importing persons shall include any company or association or body of individuals, whether incorporated or not.
5) Terms and expression not herein defined shall have the meanings assigned to them in the contract Act, 1872 (as amended) or the Sale of Equipment Act, 1930 (as amended) or the General Clauses Act, 1897 (as amended) or of INCOTERMS, (current edition published by the International Chamber of Commerce, Paris) as the case may be.
6) Any reference to ‘Equipment’ shall be deemed to include the complete work i.e. delivery, installation, testing, training, commissioning & warranty.
7) Any reference to ‘Contract’ shall be deemed to include all other documents) as described in GCC-clause 2.5.
8) Any reference to any Act, Government Policies or orders, CCA guidelines, WebTrust and CAB forum shall be deemed to include all amendments to such instruments, from time to time.

1.2 Definitions

In the contract, unless the context otherwise requires:

1) "bid" (including the term ‘tender’, ‘offer’, ‘quotation’ or ‘proposal’ in specific contexts) means an offer to supply Equipment, services or execution of works made as per the terms and conditions set out in a document inviting such offers.

2) "Bidder” (including the term 'Bidder', ‘Successful Bidder’, ‘Contractor’, ‘System Integrator’, or 'service provider' in specific contexts) means any person or company, every artificial juridical person not falling in any of the descriptions of bidders stated herein before, including any agency branch or office controlled by such person, participating in a Tender Process.

3) Bill of Materials” (including the term Financial Bid (BOM)) means the financial sheet and complete Bill of Quantities forming part of the bid.

4) "Commercial Bank" means a bank, defined as a scheduled bank under section 2(e) of the Reserve Bank of India Act, 1934.

5) “Consignee” means the person to whom the Equipment are required to be delivered as stipulated in the contract or intimated at later date.

6) “Contract” means and includes ‘Contract issued from NIXI Portal’, ‘Purchase Order’ or ‘Supply Order’ or ‘Withdrawal Order’ or ‘Work Order’ or , or‘ Agreement’ or a ‘repeat order’ accepted/ acted upon by the contractor or any amendment thereof, or a ‘formal agreement’, under specific contexts;

7) “Bidder/Contractor/ Successful Bidder” (including the terms ‘Supplier’ or ‘Service Provider’, ‘System Integrator’, or ‘Firm’ or ‘Vendor’ or ‘Bidder’ under specific contexts) means the person, firm, company, with whom the contract is entered into and shall be deemed to include the contractor's successors (which is/are approved by the NIXI), representatives, heirs, executors, and administrators as the case may be unless excluded by the terms of the contract.;

8) “Day”, “Month”, “Year” shall mean calendar day/ month or year (unless reference to financial year is clear from the context).

9) “General Conditions” means the General Conditions of Contract, also referred to as GCC.

10) "Equipment/ Equipment & Services" (including the terms items, equipment, Services in specific contexts). Any reference to Equipment shall be deemed to include hardware, software and specific services that are Installation, Commissioning, Training, Testing, Acceptance, Operations and Maintenance etc.

11) “Government" means the Central Government or a State Government as the case may be and includes Autonomous Bodies, agencies and Public Sector Enterprises under it, in specific contexts;

12) “NIXI” means National Internet Exchange of India, who is in the process of procurement of Equipment and services laid down in this tender document. O/o NIXI and O/o CCA are end user of this project.

13) “Inspection” means activities such as measuring, examining, testing, analyzing, gauging one or more characteristics of the Equipment or services or works, and comparing the same with the specified requirement to determine conformity.

14) “Intellectual Property Rights” (IPR) means the rights of the intellectual property owner concerning a tangible or intangible possession/ exploitation of such property by others. It includes rights to Patents, Copyrights, Trademarks, Industrial Designs, Geographical

indications (GI).

15) **“**Parties”: The parties to the contract are the "Contractor" and the NIXI, as defined in this clause;

16) “Performance Security” (includes the terms ‘Security Deposit’ or ‘Performance Bond’ or ‘Performance Bank Guarantee’ or other specified financial instruments in specific contexts) means a monetary guarantee to be furnished by the successful Bidder or Contractor in the form prescribed for the due performance of the contract;

17) “Location of Delivery” the delivery location of the Equipment shall be deemed to take place on delivery of the Equipment, at following places (as defined in Section-IV-BoM) asper the terms and conditions of the contract -

18) “Consignee” The consignee at his premises; or the consignee at the destination station in case of a contract stipulating for delivery of Equipment at the destination station.

19) “Procurement” (or ‘Purchase’, or ‘Government Procurement/ Purchase’) means the acquisition of Equipment/ Services/ works by way of purchase, either using public funds or any other source of funds (e.g. grant etc.) of Equipment, works or services or any combination thereof, by NIXI, the term “procure”/ “procured” or “purchase”/ “purchased” shall be construed accordingly;

20) “The Procuring Entity/Organization” means NIXI in its capacity as Implementing agency of NIXI procuring Equipment & Services;

21) “Procurement Officer” means the officer dealing the project issuing the Tender Document, Purchase order from NIXI and/or the signing contract or etc. on behalf of the NIXI;

22) “Specification” or “Technical Specification” means the drawing/ document/ standard/Datasheets or any other details governing the supply of Equipment or performance of services that prescribes the requirement to which Equipment or services have to conform as per the contract.

23) “Signed” means ink signed or digitally signed with a valid Digital Signature as per IT Act 2000 (as amended from time to time). It also includes stamped, except in the case of Letter of Award or amendment thereof.;

24) “Tender”; “Tender Document”; “Tender Enquiry” or “Tender Process”: ‘Tender Process’ is the whole process from the publishing of the Tender Document till the resultant award of the contract. ‘Tender Document’ means the document (including all its sections, appendices, forms, formats, etc.) published by the NIXI on NIXI Website to invite bids in a Tender Process. The Tender Document and Tender Process may be generically referred to as “Tender" or "Tender Enquiry", which would be clear from context without ambiguity.

25) “Tender No./ xxxx” refers to the NIXI Bid Number, Bidders should add this number same as NIXI Bid Number in all documentation pertaining to this tender.

26) “NIXI Portal”; NIXI website on which this tender will be hosted and other tender related activities will be performed.

27) “Central Sites/ Central Location”; Data Centers location in this bid, one will be used as Primary Data Center (DC) and another will be as Disaster recovery Data Center (DR). DC and DR sites will be connected dedicated leased lines.

Abbreviations:

Abbreviation	Definition
AMC	Annual Maintenance Contract
BOM	Bill of Materials (Price Schedule)
BSD	Bid Securing Declaration
CGST	Central Equipment and Services Tax
CMC	Comprehensive Maintenance Contract
DC	Primary/ Main Data Center
DR	Disaster Recovery Data Center
DSC	Digital Signature Certificate
DPIIT	Department for Promotion of Industry and Internal Trade
e-RA	Electronic Reverse Auction
EFT/ NEFT	(National) Electronic Funds Transfer
GCC	General Conditions of Contract
NIXI	National Internet exchange of India
NIXI ATC	NIXI Additional Terms and Condition
NIXI GTC	NIXI General Terms and Conditions
NIXI STC	NIXI Standard Terms and Conditions
GST	Equipment and Services Tax
IEM	Independent External Monitor
IPR	Intellectual Property Rights
INR	Indian Rupee
ITB	Instructions To Bidders
MII	Make in India

MSE	Micro and Small Enterprises
MSME	Micro, Small and Medium Enterprises
MPLS	Multi-Protocol Label Switching
NIT	Notice Inviting Tender
NMS	Network Management System/software
OEM	Original Equipment Manufacturer
PAN	Permanent Account Number
PC	(Indian) Penal Code
P.O	Purchase Order
SC	Scheduled Caste
SITC	Supply, Installation, Testing & Commissioning
TIA	Tender Inviting Authority

2 The Contract

2.1 Language of Contract

The contract shall be written in the Official Language or English. All correspondence and other contract documents, which the parties exchange, shall also be written/ translated accordingly in that language. For purposes of interpretation of the contract, the English documents/ translation shall prevail.

2.2 The Entire Agreement

The Contract to be issued on NIXI and its related documents constitutes the entire agreement between the NIXI and the contractor.

2.3 Severability

If any provision or condition of this Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of this Contract.

2.4 Parties

The parties to the contract are the contractor and the NIXI, as defined in GCC-clause 1.2 above and nominated in the contract.

2.5 Contract Documents

The following conditions and documents shall be considered to be an integral part of the contract, irrespective of whether these are not appended/ referred to in it. Any generic reference to ‘Contract’ shall imply reference to all these documents as well:

1) Contract issued by NIXI.
2) Valid and authorized Amendments issued to the contract.
3) Final written submissions made by the contractor during negotiations, if any;
4) NIXI (GTC i.e. General Terms and Conditions)
5) NIXI (STC i.e. Special Terms & Conditions & ATC i.e. Additional Terms & Conditions) if any
6) the contractor’s bid;
7) Forms and Formats signed and submitted by bidder
8) Integrity Pact
9) Non-Disclosure Agreement (NDA)
10) Modifications/ Amendments, Waivers and Forbearances
11)Tender Document and its amendment/Corrigendum

2.5.1 Modifications/ Amendments of Contract

1) If any of the contract provisions must be modified after the contract issued, the modifications shall be made in writing and signed by the NIXI, and no modified provisions shall be applicable unless such modifications have been done. No variation in or modification of the contract terms shall be made except by a written amendment signed by the NIXI. Requests for changes and modifications may be submitted in writing by the contractor to the NIXI. At any time during the currency of the contract, the NIXI may suo-moto or, on request from the contractor, by written order, amend the contract by making alterations and modifications within the general scope of the Contract.

2) If the contractor does not agree to the suo-moto modifications/amendments made by the NIXI, he shall convey his views within 10 days from the date of amendment/ modification conveyed. Otherwise, it shall be assumed that the contractor has consented to the amendment.

3) Any verbal or written arrangement abandoning, modifying, extending, reducing, or supplementing the contract or any of the terms thereof shall be deemed conditional and shall not be binding on the NIXI unless and until the same is incorporated in a formal instrument and signed by the NIXI, and till then the NIXI shall have the right to repudiate such arrangement

2.5.2 Waivers and Forbearances

The following shall apply concerning any waivers, forbearance, or similar action taken under this Contract:

1) Any waiver of NIXI's rights, powers, or remedies under this Contract must be in writing, dated, and signed by an authorized representative of the NIXI granting such waiver and must specify the terms under which the waiver is being granted.

2) No relaxation, forbearance, delay, or indulgence by NIXI in enforcing any of the terms and conditions of this Contract or granting of an extension of time by NIXI to the contractor shall, in any way whatsoever, prejudice, affect, or restrict the rights of NIXI under this Contract, neither shall any waiver by NIXI of any breach of Contract operate as a waiver of any subsequent or continuing breach of Contract.

3 Governing Laws and Jurisdiction

1) This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Laws of India for the time being in force.

2) Irrespective of the place of delivery, or the place of performance or the place of payments under the contract, the contract shall be deemed to have been made

at the place from which the Contract/Purchase Order or the contract Agreement has been issued. The courts of such a place (i.e New Delhi) shall alone have jurisdiction to decide any dispute arising out or in respect of the contract.

4 Communications

4.1 Communications

1) All communications under the contract shall be served by the parties on each other in writing (Letter/email), in the English language, and served in a manner customary and acceptable in business and commercial transactions.
2) The effective date of such communications shall be either the date when delivered to the recipient or the effective date mentioned explicitly in the communication, whichever is later.
3) No communication shall amount to an amendment of the terms and conditions of the contract, except a formal letter of amendment of the contract, so designated.
4) Such communications would be an instruction or a notification or an acceptance or a certificate from the NIXI, or it would be a submission or a notification from the contractor.

4.2 The person signing the Communications

For all purposes of the contract, there under all communications to the other party shall be signed by:

1) The Authorize signatory on behalf of the contractor shall sign all correspondences.
2) the Procurement Officer signing the contract shall administer the contract and sign communications on behalf of the NIXI. consignees; Project executing officer; Inspecting officers and the paying authorities mentioned in the contract shall also administer respective functions during Contract Execution.

4.3 Address of the parties for sending communications by the other party.

1) For all purposes of the contract, including arbitration, thereunder the address of parties to which the other party shall address all communications and notices shall be:
   a) The address of the contractor as mentioned in the contract unless the contractor has notified the change of address by a separate communication containing no other topic to the NIXI. The Contractor shall be solely responsible for the consequence of an omission to notify a change of address in the manner aforesaid, and
   b) The address of the NIXI shall be the address mentioned in the contract. The contractor shall also send additional copies to officers of the NIXI presently dealing with the contract.
   c) In case of the communications from the contractor, copies of communications shall be marked to the Procurement Officer signing the contract, and as relevant also to Inspecting Officer; Project executing officer; interim/ ultimate consignee and paying authorities mentioned in the contract. Unless already stipulated in the contract before the contract's start, the NIXI and the contractor shall notify each other if additional copies of communications are to be addressed to additional addresses.

5 Contractor's Obligations and restrictions on its Rights

5.1 Changes in Constitution/ financial stakes/ responsibilities of a Contract's Business

The Contractor must proactively keep the NIXI informed of any changes in its constitution/ financial stakes/ responsibilities during the execution of the contract.

5.2 Obligation to Maintain Eligibility and Qualifications

The contract has been awarded to the contractor based on specific eligibility and qualification criteria. The Contractor is contractually bound to maintain such eligibility and qualifications during the execution of the contract. Any change which would vitiate the basis on which the contract was awarded to the contractor should be pro-actively brought to the notice of the NIXI within 7 days of it coming to the Contractor's knowledge. These changes include but are not restricted to the Change regarding declarations made by it in it bid in Form 1.2: Eligibility Declaration

5.3 Consequences of a breach of Obligations

Should the contractor commit a default or breach of GCC-clause 5.1 to 5.7, the Contractor shall remedy such breaches within 21 days, keeping the NIXI informed. However, at its discretion, the NIXI shall be entitled, and it shall be lawful on his part, to treat it as a breach of contract and avail any or all remedies thereunder. The decision of the NIXI as to any matter or thing concerning or arising out of GCC-clause 5.1 to
5.7 or on any question whether the contractor or any partner of the contractor firm has committed a default or breach of any of the conditions shall be final and binding on the contractor.

5.4 Assignment and Sub-contracting

1) All the manpower to be deployed in project for delivery, installation, testing & commissioning and resident engineer, technical support and maintenance including onsite support should be on the payroll of the bidder/Contractor or OEM equipment offered. Outsourcing of manpower will not be allowed.

2) the contractor shall not sublet, transfer, or assign the contract or any part thereof or interest therein or benefit or advantage thereof in any manner whatsoever.

3) the contractor shall take prior permission in writing from NIXI for any sub- contracting that contractor wish to enter into for limited Works (e.g. loading/unloading, racking and stacking of equipment(s) etc.).

4) If the Contractor sublets or assigns this contract or any part thereof without such permission, the NIXI shall be entitled, and it shall be lawful on his part, to treat it as a breach of contract and avail any or all remedies thereunder.

5.5 Indemnities for breach of IPR Rights or from other issues

1) the contractor shall indemnify and hold harmless, free of costs, the NIXI and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses,

which may arise in respect of the Equipment provided by the contractor under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:

a) any design, data, drawing, specification, or other documents or Equipment provided or designed by the contractor for or on behalf of the NIXI.
b) The installation of the Equipment by the contractor or the use of the Equipment at the NIXI other sites of NIXI.

2) If any proceedings are brought, or any claim is made against the NIXI arising out of the matters referred above, the NIXI shall promptly give the contractor a notice thereof. At its own expense and in the NIXI's name, the contractor may conduct such proceedings and negotiations to settle any such proceedings or claim, keeping the NIXI informed.

3) If the contractor fails to notify the NIXI within twenty-eight (28) days after receiving such notice that it intends to conduct any such proceedings or claim, then the NIXI shall be free to conduct the same on its behalf at the risk and cost to the contractor.

4) At the contractor's request, the NIXI shall afford all available assistance to the contractor in conducting such proceedings or claim and shall be reimbursed by the contractor for all reasonable expenses incurred in so doing.

5) The Contractor shall be solely responsible for any damage, loss or injury which may occur to any property or to any person by or arising out the execution of the works or temporary works or in carrying out of the contract otherwise than due to the matters referred to in this agreement hereinbefore. The contractor would ensure for observance of all labor and other laws applicable in the matter and shall indemnify and keep indemnified the NIXI, end users/ its customers against the effect of non- observance of any such laws.

5.6 Confidentiality and IPR Rights

5.6.1 IPR Rights

All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the contractor under this Contract shall become and remain the property of the NIXI and must not be shared with third parties or reproduced, whether in whole or part, without the NIXI's prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the NIXI, together with a detailed inventory thereof**.**

5.6.2 Confidentiality

All documents, drawings, samples, data, associated correspondence or other information furnished by or on behalf of the NIXI to the contractor, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract, are confidential and shall remain the property of the NIXI and shall not, without the prior written consent of NIXI neither be divulged by the contractor to any third party, nor be used by him for any purpose other than the design, procurement, or other services and work required for the performance of this Contract. If advised by the NIXI, all copies of all such information in original shall be returned on completion of the contractor's performance and obligations under this contract.

5.6.3 Obligations of the contractor

1) Without the NIXI's prior written consent, the contractor shall not use the information mentioned above except for the sole purpose of performing this contract.
2) The contractor shall treat and mark all information as confidential and shall not, without the written consent of the NIXI divulge to any person other than the person(s) employed by the contractor in the performance of the contract. Further, any such disclosure to any such employed person shall be made in confidence and only so far as necessary for such performance for this contract.
3) Notwithstanding the above, the contractor may furnish to its holding company such documents, data, and other information it receives from the NIXI to the extent required for performing the contract. In this event, the contractor shall obtain from such holding company an undertaking of confidentiality similar to that imposed on the contractor under the above clauses.
4) The obligation of the contractor under sub-clauses above, however, shall not apply to information that:
   a) now or hereafter is or enters the public domain through no fault of Contractor;
   b) can be proven to have been possessed by the contractor at the time of disclosure and which was not previously obtained, directly or indirectly, from the NIXI; or
   c) otherwise lawfully becomes available to the contractor from a third party that has no obligation of confidentiality.
5) The above provisions shall not in any way modify any undertaking of confidentiality given by the contractor before the date of the contract in respect of the contract/ the Tender Document or any part thereof.
6) The provisions of this clause shall survive completion or termination for whatever reason of the contract.

5.7 Performance Bond/ Security

1) The successful bidder shall submit a Performance Security of 5% of total value of Contract within 14 days from the date of issuance of contract. The Performance Security in the form of Bank Guarantee, Fixed Deposit and Insurance Surety bond should be valid for a minimum period of 66 months. The Performance security shall be shall be submitted in one of the following forms:
   a. Insurance Surety Bonds/ Account Payee Demand Draft/Fixed Deposit Receipt from a Commercial bank/Bank Guarantee from a Commercial bank or online Payment (Account details given below).

1.	Beneficiary Name & Address	
2.	Bank Name	
3	Bank Branch & Address	
4	Beneficiary Account No	
5	IFSC code	

The performance security must be routed through Structured Financial Messaging System (SFMS) from issuing Bank to our Bank as given above by sending IFN 760 COV Bank Guarantee Advice Message.

b. Bank Guarantee should be issued by a scheduled commercial bank in India in the prescribed form provided in Format 1.1.

2) If the contractor, having been called upon by the NIXI to furnish Performance Security, fails to do so within the specified period, it shall be lawful for the NIXI at its discretion to annul the award and enforce Bid Securing Declaration (in lieu of forfeiture of the Bid Security), besides taking any other administrative punitive action.

   (a) If the contractor during the currency of the Contract fails to maintain the requisite Performance Security, it shall be lawful for the NIXI at its discretion to terminate the Contract for Default besides availing any or all contractual remedies provided for breaches/ default, or

   (b) without terminating the Contract:

   recover from the contractor the amount of such security deposit by deducting the amount from the pending bills of the contractor under the contract or any other contract with the NIXI, or treat it as a breach of contract and avail any or all contractual remedies provided for breaches/ default.

3) Contractor needs to extend the validity of Performance Security as and when asked by NIXI due to Extension of project timelines or if any other valid reason.

4) In the event of any amendment issued to the contract, the contractor shall furnish suitably amended value and validity of the Performance Security in terms of the amended contract within fourteen days of issue of the amendment.

5) The NIXI shall be entitled, and it shall be lawful on his part, to deduct from the performance securities or to forfeit the said security in whole or in part in the event of:

   any default, or failure or neglect on the part of the contractor in the fulfilment or performance in all respect of the contract under reference or any other contract with NIXI or any part thereof for any loss or damage recoverable from the contractor which the NIXI may suffer or be put to for reasons of or due to above defaults/ failures/ neglect.

6) Subject to the sub-clause above, the NIXI shall release the performance security without any interest to the contractor on completing all contractual obligations at the satisfaction of NIXI, including the warranty obligations.

7) No interest will be payable by NIXI on any security deposit, amount forfeited, liquidated damages, SLA penalty, amount withheld any delayed payment by NIXI.

5.8 Permits, Approvals and Licenses

Whenever the supply of Equipment and Services requires that the contractor obtain permits, approvals, and licenses from local public authorities, it shall be the contractor's sole responsibility to obtain these and keep these current and valid.

6 Scope of Work & Technical Specifications:

The main objective of this project is to design, establish, operate and maintain CCA SSL root and SSL CA setups and obtain WebTrust certification along with incorporation of CCA root for SSL in all major web browsers.

The scope of works includes following:

i. To Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browser and UAT (User Acceptance Test) setup as per WebTrust compliance.

ii. Implementing the best set of practices and process flow for complete set of RCAI & CA operational activities in full compliance to all the applicable provisions of WebTrust, CAB Forum, CCA Guidelines and IT Act.

iii. To provide complete solution including detailed bill of material for hosting the OCSP and services under RCAI operations. OCSP infra should also be taken into consideration for WebTrust audit process.

iv. The proposed Root CCA/CAs SSL certificates application software should provide all the modules for SSL certificate lifecycle management like creation, suspension, revocation etc. and should also cater the requirements as specified by CCA from time to time. Bidder will submit complete Exit/Transition Management solution for exiting the contract on completion of the contract period or before for discontinuation for whatever reasons.

v. Setting up of Registration Authority (RA) for issue of SSL certificates at CA and development and maintenance of required websites for user to submit applications for SSL certificate and its integration with complete solution. Prior to issue of SSL certificates, solution should mean for Organization Validation (OV) and Domain Validation (DV).

vi. To provide the architecture diagram appropriate to suit WebTrust requirements and deploy the systems to cater to High Availability, RPO and RTO requirements of CCA India and NIXI.

vii. To supply, test, install, commission, operate and maintain equipment as per Bill of Materials (BoM) given in Section IV. The software includes operating systems (OS), antivirus software, Database software, virtualization software, back-up software, application software (including various modules as per operational requirement of RCAI) etc required for setting up CCA root and NIXI CA for issue of SSL certificate. The equipment include servers, storage, load balancer, routers, switches, firewall, HSM, Tape drives, Tapes etc. The bidder may quote additional items, if required with price break-up to complete the solution for WebTrust certification.

viii. List of services/documentations to be submitted for WebTrust Certification

S. No.	Service	Description

i	Product Setup and implementation	For all the products part of this project scope including production, DR and Test/staging/QA including hardware setup (VM software, network equipment and security devices as recommended)
ii.	CA Documentation Activities	Support for preparation of CA documentation towards policies & procedures to meet WebTrust compliance requirements - Document readiness review - CP/CPS/PDS creation - -BCP/DR documentation - Risk Assessment documentation - -Security policies & procedure - - Register templates
iii.	Readiness Assessments	For setting up of CA towards Go Live - Infrastructure readiness review including environment, hardware, network, software solutions - CA readiness review with gap assessment of policies, procedures & documentation
iv.	Compliance Activities	Towards successful compliance of WebTrust - Support for Internal audits - Support for external audits - Support for resolution of audit findings
v.	Other Reviews	For any other allied reviews and consultancy in the process of taking CA setup to Go Live
vi.	Key Generation Ceremony	Support of Key generation ceremony & all the activities there-in
vii	Operational Training	Onsite-2 business month-trainer
viii	Technical Training	Onsite-Sr. Consultant (5 Days)-based on location.

ix. To implement Web Trust compliant solution architecture for complete operation s for issue of SSL certificate to obtain a seal of WebTrust/EV-WebTrust from the certified firm/ practitioner/accountant who are licensed and proven track record by AICPA/CICA.

x. To get WebTrust certification for incorporating CCA root certificate for SSL in all major web browser namely Chrome, Mozilla, MS Edge, Safari etc.

xi. To submit a concept document on compliances requirement with the latest version of the Guidelines for the Issuance and Management of Extended Validation Certificates.

xii. Detailed bar chart depicting the time schedule for indicating the start and end time of individual activities being identified by the bidder in the complete process. Note: i. For the purpose of understanding the existing service requirement, the prospective bidders may visit primary and secondary sites hosted at DC and DR sites of NIXI (at Delhi NCR and Bangalore only).

xiii. Supply of manpower for operation and maintenance for 5 years as per detail given below. The cost of manpower is to be quoted on per year basis:

Description	**No of Resources**
System Administrator	1
Network Administrator	1

PKI Administrator	1
Security Officer	1
CA Administrator	1

However, the bidder will deploy manpower for the support required to meet the SLA, and cost of which will be included in their support price in BoM.

xiv. The bidder shall be required to visit the Data Centers for Primary and DR sites before submitting the bids to suggest the layout of the Data Centre requirement and quote additional items for making the RCAI operation for issue of SSL certificate to be WebTrust compliant. These items will not be considered for deciding L1 and hence not part of the BOM.

xv. The bidder has to also assess and suggest point to point bandwidth between Primary DC in Delhi NCR and DR site in Bengaluru.

xvi. The proposed solution should also meet the requirements mentioned under the IT Act, Rules (Schedule II & Schedule III), regulation and standards, CCA guidelines as applicable in addition to WebTrust requirements. The basic WebTrust requirements are mentioned here:

#	Category	Description	Justification/ References	WebTrust reference URL
1	Network isolation (Requirement of separate zones)	The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum. The WebTrust principles states that the CA services should be categorized based on the criticality of the application	Principle 4: Network and Certificate System Security Requirements (Section 1.1 to 1.12)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7
2	Services isolation	Database needs to be limited to authorized individuals, applications and services only	1. Principle 3: CA Environmental Security (Section 8 2. Principle 4: Network and Certificate System Security Requirements (Section 1.5)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7

3		Root CA and Issuing CA systems needs to be separated	Principle 4: Network and Certificate System Security Requirements (Section 1.3 and 1.5)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7
4		Certificate Management Systems and it is associated service security	Principle 4: Network and Certificate System Security Requirements (Section 1.4 and 1.5)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7
5		OCSP requirement of making online 24/7. Since this is depended on the database for the getting the Certificate status, resource and high availability needs to be maintained by CA.	Principle 2: SSL Service Integrity (Specifically Section 5.7 and refer it section 5.5 to 5.10)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7
6		Direct exposure of Certificate management system to public is allowed and it requires connectors for consuming the external services like Certificate Transparency submission. Certificate Transparency is a log server where Pre-certificates needs to be submitted to at least 3 CT log operators. This is the same for OCSP where HSM will be placed in the Highly secured zone. So an Internal application needs to be in place for speaking to Publically exposed application to provide the services	Principle 4: Network and Certificate System Security Requirements (Section 1.1 to 1.12)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7
7	Redundancy architecture	Any Failure in above systems need to raise an incident with Mozilla and will be put forth in a public discussion where all other CA's will be part of this discussion. The incident can be any type miss-issuances, CA service going down etc. This can lead to delisting from the root operators if the discussion	1. In Mozilla Section 2.4 Incidents 2. In Chrome policy section 7 responding to incidents	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ https://www.chromium.org/Home/chromium-security/root-ca-policy/

		is not provided with the proper justifications and if any malicious behaviour is identified by the operators		
8		Merging of the other services like OCSP will affect the Certificate issuing system to fail because these 2 are the high transaction applications. So the proper isolation of the applications and it security needs to be provided.	Principle 4: Network and Certificate System Security Requirements (Section 1.3 and 1.5)	https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216wtbr-26-rev-august-2022final.pdf?la=en&hash=D96D591D9422E73871B83488D275B9FB78DD1FD7

xvi: The WebTrust check list is given as Annexure I.

The bidder may also refer WebTrust document at https://www.cpacanada.ca/-/media/site/operational/ep-education-pld/docs/mds21216webtrustca-222final-(15).pdf?la=en&hash=9355E6E558FE7924BEEAF5FF501B486D6903C339

xvii. Responsibility Matric:

Sl No	Item	Bidder/ OEM	NIXI/ CCA
1	To design, supply, install, develop, deploy and maintain software and hardware with respect to CCA India and NIXI CA setup in separate cage infrastructure in DC, DR and QA setup	√	x
2	To provide the architecture diagram appropriate to suit WebTrust requirements and deploy the systems to cater to High availability, RPO and RTO requirements of CCA India and NIXI	√	x
3	Implementing the best set of practices and process flow for complete set of RCAI operational activities in full compliance to all the applicable provisions of WebTrust	√	x
4	Implementing the web Trust compliant solution architecture for complete RCAI operations for SSL to obtain a seal of WebTrust / EV-WebTrust from the certified firm / practitioner / accountant who are licensed and proven track record by AICPA/CICA	√	x
5	Providing the state-of-art bill of material including hardware, operating software, application software (including various modules as per operational requirement of RCAI), with exact make & model, even if some of the items are missing in the Bill of Material in the Tender Document	√	x
6	To submit and implement complete solution including detailed bill of material for hosting the OCSP services under RCAI operations. OCSP infra should also be taken into consideration for web trust audit process	√	x
7	To submit acceptance test plan for DC and DR sites.	√	x
8	To suggest and implement processes for enabling CCA root to be placed in all the major browsers	√	x

9	To submit and implement a concept document on compliances requirement with the latest version of the Guidelines for the Issuance and Management of Extended Validation Certificates	√	x
10	Detailed bar chart depicting the time schedule for indicating the start and end time of individual activities being identified by the bidder in the complete process. Note: i. For the purpose of understanding the existing service requirement, the prospective bidders may visit primary and secondary sites hosted at DC and DR sites of NIXI(at Delhi and Bangalore only)	√	x
11	To develop and maintain the website for user interface for RA and integrate it with overall solution	√	x
12	To provide DC & DR Locations/Sites, seating space for team	x	√
13	To visit & provide DC & DR Sites Design, Layouts and GAPs to make it WebTrust Compliant	√	x
14	To enable the basic facility (caging, cameras, access controls, safe etc.) for DC & DR sites for WebTrust compliant	x	√
15	Monitoring & Maintenance of DC & DR Sites	√	x
16	To assess Internet/connectivity requirements for DC and DR end to end connectivity and internet connectivity at DC & DR Sites for OCSP and other services	√	x
17	To enable the needed connectivity as per design requirements (ref point 16)	x	√

6.1 Acceptance Testing (AT):

The Acceptance Test plan shall be submitted within 15 days of issuance of Contract by Contractor to NIXI for approval. AT shall be carried out jointly by Contractor and NIXI. On successful completion of AT, certificate per site shall be issued by NIXI to the contractor as per below accomplishment of work:

a. Contractor will support and configure the equipment on any secure link. Contractor shall configure the equipment(s) to establish the data transfer required between Delhi site and Bangalore site and data transfer should be secure and encrypted as per standard.

b. Contractor will carry out Vulnerability assessment (VA) and Penetration Testing (PT) using certified tool through a Third-party certified agency before acceptance, if required.

Responsibility of Contractor during Acceptance Test(AT) and commissioning is to provide below mentioned artefacts but not limited to:

i) To set up CCA SSL ROOT for NIXI along with setting up CA with WebTrust Audit for issue of SSL certificate in DC and DR Sites of NIXI in Delhi and Bengaluru. The Contractor should supply and install the hardware/software along with development of processes for WebTrust and require the following documentations but not limited to only these documents for WebTrust requirements.

i. OEM certification of all the equipment(s) installed.
ii. Low level and High-Level design
iii. Successful Vulnerability assessment (VA) and Penetration Testing (PT) report.

iv. Availability of all the defined services shall be verified.

v. Draft CA & Network security policy document as per standard to be followed as per WebTrust.

vi. Any other document/activity identified during project implementation period.

c. NIXI may require the Contractor to carry out any test and/or inspection not specified in the Contract but deemed necessary to verify that the characteristics and performance of the equipment(s) and services comply with the technical specification's codes and standards under this Contract. The Contractor shall be required to carry out such test and/or inspection at its own cost.

6.2 WebTrust Audit

Framework for auditors to assess the adequacy and effectiveness of the controls used by Certification Authorities (CAs) is based on ISO 21188 "Public Key Policy and Practices Framework"

Although these Principles and Criteria are intended to be used in the conduct of WebTrust engagement by those auditors licensed by CPA Canada., this document can be used, in conjunction with consideration of the additional compliance requirements set forth by the CA/Browser Forum for publicly-trusted CAs (i.e. Baseline Requirements, Network Security Requirements, Code Signing, Extended Validation, etc.) in the conduct of any assurance engagement or internal audits for Public PKIs.

6.3 Technical Specifications and Standards

The Equipment & Services to be provided by the contractor under this contract shall conform to the technical specifications mentioned in **`Technical Specification' under Sections V** of the Tender Document. For standards and requirements where no applicable specifications are mentioned, appropriate latest authoritative standards and quality assurance issued by the concerned institution shall be applicable. The Equipment supplied shall be:

i. Entirely brand new and unused.

ii. The hardware specifications provided in the tender is the minimum required and bidder may quote for higher specifications to optimize as per their solution requirements. The bidders should quote the products strictly as per the tendered specifications or of higher specifications giving exact make & model and specifications. All the technical literature for the products offered by the bidder may be enclosed in the bid.

iii. The bidders should give clause-by-clause compliance for the technical specification of the equipment along with cross reference of individual points from product data sheet/ literature which is to be submitted in their technical bids.

6.4 Comprehensive Warranty and Maintenance:

Supplier shall ensure comprehensive onsite support for the complete setup for a total of 5 years from date of acceptance at each site including consultancy work, all upgrades, processes, audits compliances, spares, consumables, skilled manpower etc.

The following warranty and support clauses shall apply:

6.4.1 The Equipment supplied and services rendered by the Contractor shall be in accordance with the tender specifications & quality. The Equipment(s) shall carry onsite Comprehensive Warranty and

Support for Five (5) years. The warranty period shall start from the date of successful commissioning by contractor and acceptance by NIXI for each site

6.4.2 Obligations of the contractor under the warranty and support clause will remain valid for all the sites installed, accepted and paid-for; even though the contract is terminated for any reason whatsoever.

6.4.3 OEM Warranty certificates must be submitted by Contractor at the time of acceptance of Equipment. Warranty should also reflect in the support website of the OEM if such option is provided by the respective OEMs.

6.4.4 The equipment to be ordered through P.O/Contract are meant to be deployed across various location across country. In case any of the installed / non-installed equipment(s) are shifted from one location to another then in such a case contractor shall be responsible to provide warranty, support, maintenance and RMA (Return Merchandise Authorization) at such locations also.

6.4.5 **Retention Policy:** Since the equipment(s) to be deployed in a security projects; therefore, data privacy shall be ensured through Storage Retention Policy i.e. NIXI shall retain the faulty storage disks/media/memory in case of any replacement during the maintenance. In case of replacement of device/equipment, NIXI shall retain all the storage disks (faulty or otherwise). No additional cost will be paid for any retained storage disks.

6.4.6 In case of any rectification of a defect or replacement of any defective Equipment during the warranty period, the warranty for the rectified/ replaced Equipment shall remain till the original warranty period and same should reflect on OEM’s website with revise equipment details, if such facility available with OEM.

6.4.7 All ongoing software upgrades for all major and minor releases should be provided during the complete warranty and support period.

6.4.8 All types of support (hardware trouble shooting, maintenance etc.) at sites will be provided by the Contractor.

6.4.9 OCSP service support shall be made available on 24x7 basis.

6.4.10 Business Continuity, RTO & RPO :

The business continuity design of DC and DR facilities must cater to high availability and should ensure RPO (Recovery Point Objective) of not more than 5 minutes and RTO (Recovery Time Objective) of maximum 2 hours.

As a process, new certificates may be issued after new certificates are reflected in DR servers so as to ensure no loss of certificates issued to end users.

6.4.11 **Manpower for maintenance:** Contractor will deploy two resident engineers during business hours (09.00 am to 06.00 pm) from Mon to Saturday (i.e 6 days a week) at specified location i.e Bengaluru and/or Delhi from the date of acceptance of sites. Deployed manpower shall be exclusive for these sites and shall remain available on call during non official hours for remote and onsite emergency support. The Deployed manpower must have B.Tech/MCA degree with CCNA/JNCIA or equivalent certifications and minimum experience of three years on subject matter (i.e on installed hardware and software in data center environment). The Resident Engineers as asked in the tender should be on direct muster-roll (pay-roll) of the Contractor.

Compliance with relevant applicable laws including but not limited to provident fund, ESI etc. needs to be ensured by the contractor. An undertaking to this effect should be submitted by the Contractor. The roles and responsibilities of manpower is to monitor, manage, supplied hardware etc. procured under the project's scope including the monthly / weekly reports or any other project related work assigned by NIXI. Payment for manpower will be made based on the number of days of actual attendance. In addition, Penalty @ Rs. 5000/- per day will be imposed on each day absence of each manpower.

6.4.12 **Uptime of installed Equipment(s) and Applications:** The contractor shall arrange for regular upkeep and maintenance of the equipment to keep the equipment and applications running to its optimal capacity. The contractor shall be required to maintain the installed system till the completion of warranty and support period of individual site through its nearest support center. In case of fault, Resident Engineer/ NIXI will log complain to contractor's toll-free number/ web support system. Complaint shall be responded with 2 hours and resolved within 4-8 hrs from the time of call logged in business hours (i.e. 09.00am to 06.00 pm). This will be termed as a permissible time per site.

Overall Uptime of SSL Services Availability (> 99.982%, calculated on quarterly basis) shall be ensured by the supplier (including hardware, software and applications).

6.4.13 **Penalty:** In case of Data Transfer or applications gets interrupted, due to fault at Site in equipment (s))/ or applications for any reasons attributable to supplied equipment(s) and services under warranty and support period , Penalty @ 0.25 % of total equipment(s) value per site per day or part thereof will be deducted beyond permissible limits. In case of equipment faults persist for more than 72 hours, Penalty @ 0.5 % of total equipment value per site per day or part thereof the day will be deducted. In case, any site goes down more for than fifteen (15) days, NIXI may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.

Any loss of uptime below the level as defined above shall invoke penalty@ 5000/- for each 0.01% loss of uptime. Uptime shall be calculated quarterly.

Total penalties will not exceed 12.5% of total contract value. Penalties will be deducted from due payment/performance securities.

6.4.14 **Change Management:** The contractor shall obtain prior approval at least two weeks before changing their workforce personnel's and other resources during the course of on-going assignment. Contractor shall ensure that there is proper knowledge transfer as well as handing over of necessary resources to avoid any kind of adverse impacts to the work during the transition of resources.

6.4.15 **Trainings & Technical Documentation**: Comprehensive operations and technical trainings shall be provided by the Supplier & OEM to NIXI and CCA nominated team members during the period of contract for smooth operations. Four sets of hard copies of technical and operations manuals along with soft copy covering all aspects of installation, testing, maintenance, operations, training, audits, compliances and commissioning shall be handed over to NIXI and CCA before acceptance testing. Any new changes during the contract period in the above documentations shall be promptly notified to NIXI and CCA

7 Inspection and Quality Assurance

7.1 Tests and Inspections

NIXI or its representative shall have the right to inspect or to test the Equipment to confirm their conformity to the ordered specifications. The supplier shall provide all reasonable facilities and assistance to the inspecting authority at no charge to NIXI. In case any inspected or tested equipment fail to conform to the specifications, NIXI may reject them and supplier shall replace the rejected equipment with the equipment in conformity with the specification required free of cost to NIXI.

7.2 Consequence of Rejection

Upon the Equipment being rejected by the NIXI, the NIXI shall be at liberty to:

1) Demand that such stores shall be removed by the contractor at his cost subject as hereinafter stipulated, within 15 days of the date of intimation of such rejection. The decision of the NIXI in this regard shall be final in all respects. The Contractor shall bear all cost of such replacement, including taxes and freight, if any, on replacing and replacing Equipment without being entitled to any extra payment on that or any other account. NIXI will not return the Hard Disk from used systems.

7.3 NIXI's right of Rejection of Inspected Equipment

1) Equipment accepted by the NIXI and/ or its inspector at the initial inspection and final inspection in terms of the contract shall in no way dilute the NIXI's right to reject the same later if found deficient concerning 'Technical Specifications'.

2) Notwithstanding any approval which the NIXI may have given in respect of the Equipment or any materials or other particulars or the work or workmanship involved in the performance of the contract and notwithstanding delivery of the Equipment, it shall be lawful for NIXI, to inspect, test and, if necessary, reject the Equipment or any part, portion or consignment thereof, after the Equipment' arrival at the final destination within a reasonable time after actual delivery thereof at the delivery locations mentioned in the contract, if such Equipment or part, portion or consignment thereof is not in all respects in conformity with the terms and conditions of the contract whether on account of any loss, deterioration or damage before dispatch or delivery or during transit or otherwise howsoever.

8 Transfer of Assets and Insurance

8.1 Transfer of Assets

The ownership of the supplied Equipment along with its warranty and all other associated rights shall be transferred within 30 days to O/o NIXI, after successful Commissioning by contractor and Acceptance of sites by NIXI. All the risks, responsibilities, liabilities thereof in respect of all equipment at each site shall remain with contractor till handover to O/o NIXI. All licenses are to be provided in the name of Controller of Certifying Authorities/NIXI. Contractor shall provide following documents during handover of assets for individual sites:

1) Invoices with serial no of devices
2) Bill of Material
3) OEM Warranty certificates
4) Duly received Delivery challan of locations

5) Software license detail, if any
6) Acceptance reports
7) Any other document specified by NIXI

8.2 Insurance

The Bidder shall also arrange to get equipment insured to cover loss/damage due to theft, burglary, fire, or any natural disaster for the period till 365 days after successful acceptance as defined in terms of delivery in this tender document. Bidder shall be required to extend the insurance period in case, there is delay in commissioning & acceptance of project. The insurance shall not be for an amount less than 100 percent of the value of the equipment as mentioned in the Contract.

9 Terms of Delivery and delays

Delivery means Delivery, installation, testing & commissioning of supplied equipment(s) unless stipulated otherwise.

9.1 Effective Date of Contract

The effective date of the contract shall be the date on which PO has been issued by NIXI. The dates of deliveries shall be counted from the date of contract.

9.2 Time is the Essence of the contract

The time for and the date for delivering the Equipment stipulated in the contract or as extended shall be deemed to be of the essence of the contract. Delivery must be completed not later than the date(s) so specified or extended period, if any.

9.3 Locations of Delivery

The tentative Locations where the Equipment are to be delivered is stipulated in Section IV – Bill of Material.

9.4 Terms of Delivery installation, commissioning, WebTrust Certification and Incorporation of CCA root for SSL in Major Web Browsers

1. All Equipment & Services shall be offered at site including logistics, transportation, loading/unloading, installation, testing & commissioning. Cost of the same shall be included in offer price. All aspects of safe delivery shall be the exclusive responsibility of the contractor.

2. Any changes in locations shall also be confirmed at the time of release of Purchase order/Contract. NIXI reserve the right to change of location before delivery of Equipment(s) to designated locations. However, any relocation of equipment(s) in the same city shall not be treated as change of location before equipment(s) installation. No Equipment shall be deliverable to the NIXI on Sundays and public holidays or outside designated working hours without the written permission of NIXI.

3. The contractor shall deliver the consignment at the place/ places as detailed in the Bid/contract, the quantities of the Equipment detailed therein, and the Equipment shall be delivered not later than the dates stipulated in the Bid/contract. The delivery shall not be complete unless the Equipment are inspected and accepted by the NIXI or by any designated

officer as provided in the contract.

4. The contractor fails to dispatch the Equipment before the expiry of the delivery period then contractor must apply to NIXI in writing to extend the delivery period and only if approved by the NIXI then only dispatch the balance quantity in specified delivery time limit. If the contractor delivers the Equipment without obtaining an extension, it would be doing so at its own risk, and no claim for payment for such supply and/ or any other expense related to such supply shall lie against NIXI.
5. Contractor shall complete the delivery, installation, testing and commissioning of all the equipment(s) at all sites within 60 days from the date of issuance of Contract.
6. Contractor shall ensure the WebTrust certification is obtained within 180 days from the date of issue of the contract.
7. Contractor shall ensure CCA root is incorporated in all Major Web Browsers in maximum 1 year period from date of contract.

9.5 Delay in the contractor's performance

If the contractor fails to deliver the Equipment (s) or delays in provision of Services (e.g. installation, commissioning, training, maintenance etc.) within the period fixed for such delivery in the contract or as extended or at any time repudiates the contract before the expiry of such period, the NIXI may without prejudice to his other rights:

(1) recover from the contractor liquidated damages as per clause 9.6(2) below, and/or

(2) treat the delay as a breach of contract as per GCC clause 12.1 below and avail all the remedies therein.

9.6 Extension of Delivery Period and Liquidated Damages:

1) The original Delivery Period may be re-scheduled by the NIXI without any Liquidated damages if such reschedule is warranted due to Force Majeure conditions mentioned below clause no. 9.7 and also on the ground/reasons of delay attributable to the NIXI. In all other cases, if any extension is given then same shall attract LD as given in below sub clause.
2) **Liquidated Damages (LD) for delayed delivery of equipment:** If the Contractor fails to complete delivery, installation, testing, commissioning, training, acceptance etc. of equipment(s) as per timelines specified in the contract, then in such a case NIXI would be entitled to impose the Liquidated Damages for the delay @ 0.5% of the value of total equipment(s) at non- commissioned sites per week or part of the week of delayed period. Liquidated Damages shall not exceed 10% of the total contract value. In case, delay beyond 10 weeks, NIXI may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.
3) NIXI will serve a notice duly accompanied by a preliminary calculation sheet to the contractor against whom levy of LD is proposed. In case the contractor is not satisfied/ agree with

   (i) the reason/grounds for which levying of LD is proposed and or

   (ii) method of calculation of amount of LD.

4) Contractor may submit a representation to NIXI within the stipulated timeline (as indicated in the notice i.e. 15 days) clearly mentioning his claims, ground of such claims etc. along with all the documents (self-certified) supporting his claims.

5) Waiver from LD may be considered only if the contractor submits a written representation to NIXI within the stipulated time (as indicated in the notice i.e. 15 days) on receipt of such notice of imposition of LD issued by NIXI. Decision of NIXI in the matter shall be final and binding.

9.7 Force Majeure:

1) On the occurrence of any unforeseen event, beyond the control of either Party, directly interfering with the delivery of Equipment(s) and services arising during the currency of the contract, such as war, hostilities, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts, or acts of God, the affected Party shall, within a week from the commencement thereof, notify the same in writing to the other Party with reasonable evidence thereof. Unless otherwise directed by NIXI in writing, the contractor shall continue to perform its obligations under the contract as far as reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. If the force majeure condition(s) mentioned above remains in force for 90 days or more at any time, then in such a case either party shall have the option to terminate the contract on expiry of 90 days of commencement of such force majeure by giving 14 days' notice to the other party in writing. In case of such termination, no damages shall be claimed by either party against the other, save and except those which had occurred under any other clause of this contract before such termination.
2) Notwithstanding the remedial provisions contained in GCC-clause9.6 (2) or 12.1.1, none of the Party shall seek any such remedies or damages for the delay and/ or failure of the other Party in fulfilling its obligations under the contract if it is the result of an event of Force Majeure.

10 Prices and Payments Terms:

1. Payments to contractor shall be made through Electronic Modes only. The Contractor shall provide necessary information/documents for receipt of payment through NEFT/RTGS.
2. The payments shall be subject to submission of performance security in line with the requirements specified under the Performance Security Clause. Payments shall only be made in Indian Rupees.
3. The Contractor shall submits its claim for payment in writing along with relevant documents , as stipulated in Contract and a manner as also specified therein.
4. The documents which the Contractor has to furnish while claiming payment are:
   a. Original Invoice (GST Compliant format) with serial no of each item.
   b. Delivery challan duly received (sign & Stamped from concerned officer) for all locations
   c. Insurance Certificate/policy duly assigned in favour of O/o NIXI.
   d. Licenses (software & ardware)
   e. Warranty document from OEM
   f. Any other document specified by NIXI during the course of project.

5. **The payment terms are:**

A. EQUIPMENTS (HARWARE & SOFTWARES SUPPLY INCLUDES 1st YEAR WARRANTY COST)

   a. 60 % total value of installed & accepted items at individual site on the completion of all Items Delivery, Installation, Testing, Commissioning and Acceptance per site.

   b. 20% of the total value of installed & accepted items shall become payable after obtaining WebTrust Certification.

   c. 20% of the total value of installed & accepted items shall become payable after Incorporation of CCA root in all Major Web Browsers.

B. PROFESSIONAL SERVICES (FOR 1st YEAR)

   a. 50% of professional services shall be payable after obtaining WebTrust Certification.

   b. 50% of professional services shall be payable after Incorporation of CCA root in all Major Web Browsers.

C. Professional Services (2nd year onwards), Comprehensive Support & Maintenance charges (2nd year onwards), Manpower charges (1st year onwards) of the Sites will be released on quarterly basis after completion of each quarter on pro-rata basis of the values for the complete period.

   a. NIXI will deduct LD, SLA penalty and other recoveries (if any) before releasing any payments.

   b. Delivered quantities can't exceed the quantities mentioned in the P.O. In case quantities delivered, are lower than the quantities which were required to be supplied at individual site; then in such a case NIXI reserves the right neither to accept the lower quantities and nor to make any payment for the quantities supplied.

   c. Manpower charges will be paid based on actual attendance. Attendance sheet counter-signed & stamped by the contractor will be required to enclosed with invoice. However, Contractor being principal employer shall be liable to ensure compliance with all the applicable laws pertaining to the Manpower deployed

   d. Manpower shall be properly qualified, skilled and experienced in respective areas. Manpower billing shall start after the date of acceptance of all the items supplied, installed and commissioned for the DC & DR sites upon start of CCA Root and CA operations.

6. **Fall Clause:** The bidder undertakes that he has not supplied/is not supplying the similar products, systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India and if it is found at any stage that the similar system or sub-system was supplied by the contractor to

any other Ministry/Department of the Government of India at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the contractor to the buyer, even if the contract has already been concluded. Bidder shall submit the certificate to this effect.

11 Arbitration:

1) In case any dispute or difference arises out of or in connection with or the carrying out of works (whether during the progress of the works or after their completion & whether before or after the termination, abandonments or breach of contact) except as any of the accepted matters, provided hereunder, the parties hereto, shall first endeavor to settle such disputes of differences amicably**.**

2) If both the parties fail to reach such amicable settlement, then either party (The Purchaser or Contractor) may (within 20 days of such failure) give a written notice to the other party requiring that all matter in dispute or difference be arbitrated upon. Such written notice shall specify the matters which are in difference or differences of which such written notice has been given and no other shall be reoffered to the arbitration of a single arbitrator, to be appointed by both the parties or in case of disagreement as to the appointment of a single arbitrator, to that of two arbitrators, one to be appointed by each party or in case of said arbitrators not agreeing then, to the umpire to be appointed by the arbitrators in writing before entering upon the references. Provisions of Indian Arbitration & Conciliations Act, 1996 or any statutory modification or re- enactment thereof and rules framed there under from time to time shall apply to such arbitration.

3) Venue of arbitration shall be New Delhi.

4) The arbitrators or arbitrators appointed under this Article shall have the power to extend the time to make the award with the consent of parties.

5) Pending reference to arbitration, the parties shall make all endeavors to complete the work in all respect. The disputes, if any, will finally be settled in the arbitration.

6) Upon every or any such references to the arbitration, as provided herein the cost of and incidental to the reference and Award respectively shall at the discretion of the arbitrator, or the umpire, as case may be.

7) The award of arbitrator or arbitrators, as the case may be, shall be final and binding on the parties. It is agreed that the contractor shall not delay the carrying out of the works by reason of any such matter, question or dispute being referred to arbitration, but shall proceed with the works with all due diligence. The Purchaser and the contractor hereby also agree that arbitration under this clause shall be the condition precedent to any right of action under the contract except for as provided for in the Tender.

12 Defaults, Breaches, Termination, and Closure of Contract

12.1 Termination due to Breach, Default, and Insolvency

12.1.1 Defaults and Breach of Contract

In case the contractor undergoes insolvency or receivership; neglects or defaults, or expresses inability or disinclination to honour his obligations relating to the performance of the contract or ethical standards or any other obligation that substantively affects the NIXI’s rights and benefits under the contract, it shall be treated as a breach of Contract. Such defaults could include inter-alia:

1) **Default in Performance and Obligations:** if the contractor fails to deliver any or all of the Equipment and services or fails to perform any other contractual obligations (obligation to maintain eligibility and Qualifications based on which contract was awarded) within the period stipulated in the contract or within any extension thereof granted by the NIXI.

2) **Insolvency:** If the contractor shall at any time, be adjudged insolvent or shall have a receiving order or order for the administration of his estate made against him or shall take any proceeding for composition under any Insolvency Act for the time being in force or make any conveyance or assignment of his effects or enter into any assignment or composition with his creditors or suspend payment, or

3) **Liquidation:** if the contractor is a company being wound up voluntarily or by order of a Court or a Receiver, Liquidator or Manager on behalf of the Debenture- holders is appointed, or circumstances shall have arisen which entitle the Court or Debenture-holders to appoint a Receiver, Liquidator or Manager

12.1.2 Notice for Default:

As soon as a breach of contract is noticed, a show-cause 'Notice of Default' shall be issued to the contractor, giving two weeks' notice, reserving the right to invoke contractual remedies. After such a show-cause notice, all payments to the contractor would be temporarily withheld to safeguard needed recoveries that may become due on invoking contractual remedies.

12.1.3 Terminations for Default

1) **Notice for Termination for Default:** In the event of unsatisfactory resolution of 'Notice of Default' within two weeks of its issue as per sub-clause above, the NIXI, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.

2) Such termination shall not prejudice or affect the rights and remedies, including under sub-clause below, which have accrued and/ or shall accrue to the NIXI after that.

3) Unless otherwise instructed by the NIXI, the contractor shall continue to perform the contract to the extent not terminated.

4) All warranty obligations, if any, shall continue to survive despite the termination.

12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default

If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then NIXI may take any one; or more of the following contractual remedies.

1) Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete.

2) Recover liquidated damages for delays.

3) En-cash and/ or Forfeit performance or other contractual securities.

4) Debar the contractor from participation in future procurements as follows:

   NIXI may debar the contractor or any of its successors from participating in any Tender Process undertaken by all its procuring entities for a period not exceeding two years commencing from the date of debarment

5) Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause.

6) **Risk and Cost Procurement:** In addition to termination for default, the NIXI shall be entitled, and it shall be lawful on his part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' must be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the NIXI may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the NIXI. It shall not be necessary for the NIXI to notify the contractor of such procurement. It shall, however, be at the discretion of the NIXI to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.

   Note: Regarding the Equipment which are not readily available in the market and where procurement difficulties are experienced, the period for making risk procurement shall be twelve months instead of nine months provided above.

7) Initiate proceedings in a court of law for the transgression of the law, tort, and loss, not addressable by the above means.

12.1.5 Limitation of Liability

Except in cases of criminal negligence or willful misconduct, the aggregate liability of the contractor to the NIXI, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the NIXI concerning IPR infringement.

12.2 Termination for Default/ Convenience of NIXI

12.2.1 Notice for Determination of Contract

1) The NIXI reserves the right to terminate the contract, in whole or in part for its (the NIXI's) convenience, by serving written 'Notice for Determination of Contract' on the contractor at any time during the currency of the contract. The notice shall specify that the termination is for the convenience of the NIXI of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.

2) Such termination shall not prejudice or affect the rights and remedies accrued and/ or

shall accrue after that to the Parties.

3) Unless otherwise instructed by the NIXI, the contractor shall continue to perform the contract to the extent not terminated.

4) All warranty obligations, shall continue to survive despite the termination.

12.3 Closure of Contract

12.3.1 No Claim Certificate and Release of Contract Securities

After mutual reconciliations of outstanding payments and assets on either side, the contractor shall submit a ‘No-claim certificate’ to the NIXI requesting the release of its contractual securities, if any. The NIXI shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the contractor. The contractor shall not be entitled to make any claim whatsoever against the NIXI under or arising out of this Contract, nor shall the NIXI entertain or consider any such claim, if made by the contractor, after he shall have signed a "No Claim" Certificate in favour of the NIXI. The Contractor shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof.

12.3.2 Closure of Contract

The contract shall stand closed upon

1) successful performance of all obligations by both parties, including completion of warranty obligations and final payment.

2) termination and settlements after that, if any, as per clause 12.1 or 12.2 above.

Section IV: Bill of Material (BoM) & Format for Commercial Bids

The Bill of Materials (BoM) is given below. The bidder may append additional hardware and software required if any to provide the proposed complete solution. Unit price of each item is to be provided giving break-up of base price plus applicable taxes. Please note the price are to be quoted with two digit after decimal point.

The software/hardware proposed must meet high availability and isolation requirements of WebTrust.

A. For Root SSL – CA (CCA)

For DC, DR, QA (CCA Root)							
Sl. No.	**Item Description With Make & Model**	**Certification Required/Remarks**	**Qty**	**Unit Cost**	**GST Rate in %**	**First Year Cost Inclusive of GST**	**2nd to5th Year Support Cost Inclusive of GST**
Software Components							
1	Digital Certificate Life Cycle Manager	CC EAL 4+ certified	**3**				
2	OCSP Responder	CC EAL 4+ certified					
3	Database Server	Enterprise version with perpetual license with 5 years OEM support with support for servers with cluster & replication tool bundled to set up DC, DR & QA. Database Backup with point in time recovery with 5 years OEM support	6				
4	Back Up Software	Backup and Replication software, Enterprise license	2				
5	Log Manager		2				
6	Operating System	Windows Server 2016 or higher/ Linux with appropriate support of 5 years based on solution recommended	33				
7	LDAP		2				
8	DNS		2				
9	Anti-Virus		33				
10	Data Protector Software	Software for Data Security	2				
Hardware Components:							
1	Hardware Security Module Network HSM	FIPS 140-2 level 3 certified Network HSM, minimum 500 TPS RSA-2048 signing ops	4				
2	Hardware Security Module PCI HSM	FIPS 140-2 level 3 certified PCIe type HSM, minimum 500 TPS RSA-2048 signing ops	2				

3	Servers		9				
4	Hardware Load Balancer		4				
5	Tape Drive	LTO 9	2				
6	Tape	LTO 9	10				
7	Layer 3 Switch	24 x 1 Gbps ports managed switch	4				
8	Layer 3 Switch	48 x 1 Gbps ports managed switch	4				
9	Firewall		7				
10	NTP Device	GPS Time synchronization • 19-inch1U High Rack Mount • High Stability OCXO Internal Clock Synchronization • Network Interface 1x Ethernet Ports[10/100Mbps] • 2 x 100-240V AC Power Supply Input • GPS Antenna with Mounting Kit • 90 feet Co-axial Cable with Suitable connectors	4				
11	42U Biometric Rack with camera		4				
12	Console Machine		3				
13	Router	Rack mountable router with minimum throughput of 5 Gbps with 2 no's of 10/100/1000Mbps WAN ports and two 1 Gbps LAN ports with static & dynamic routing (OSPF & BGP)	3				
Sub Total (A)							

B. For Issuing SSL – CA

For DC, DR, QA (CA)							
Sl. No.	**Item Description With Make & Model**	**Certification Required/Remarks**	**Qty**	**Unit Cost**	**GST Rate in %**	**First Year Cost Inclusive of GST**	**2nd to5th Year Support Cost Inclusive of GST**
Software Components							
1	Digital Certificate Life Cycle Manager	CC EAL 4+ certified	**3**				
2	OCSP Responder	CC EAL 4+ certified					
3	Database Server	Enterprise version with perpetual license with 5 years OEM support with support for Servers with Cluster & replication tool bundled to set up DC, DR & NDR.	6				

		Database Backup with point in time recovery with 5 years OEM support					
4	Back Up Software	Backup and Replication software, Enterprise license	2				
5	Log Manager		2				
6	Operating System	Windows Server 2019 or higher/ Linux with appropriate support of 5 years based on solution recommended	51				
7	LDAP		2				
8	DNS		2				
9	Anti-Virus		51				
10	Data Protector Software	Software for Data Security	2				
Hardware Components							
1	Hardware Security Module Network HSM	FIPS 140-2 level 3 certified, Network HSM, minimum 500 TPS RSA-2048 signing ops	9				
2	Hardware Security Module Network HSM	FIPS 140-2 level 3 certified, Network HSM, minimum 500 TPS RSA-2048 signing ops	1				
3	Hardware Security Module PCIe HSM	FIPS 140-2 level 3 certified, PCIe type HSM, minimum 500 TPS RSA-2048 signing ops	2				
4	Servers		14				
5	Hardware Load Balancer		4				
6	Tape Drive	LTO 9	2				
7	Tape	LTO 9	10				
8	Layer 3 Switch	24 x 1Gbps ports managed switch	5				
9	Layer 3 Switch	48 x 1Gbps ports managed switch	5				
10	Firewall		9				
11	NTP Device	GPS Time synchronization • 19-inch1U High Rack Mount • High Stability OCXO Internal Clock Synchronization • Network Interface 1x Ethernet Ports[10/100Mbps] • 2 x 100-240V AC Power Supply Input • GPS Antenna with Mounting Kit • 90 feet Co-axial Cable with Suitable connectors	3				

12	42U Biometric Rack with camera		6				
13	Console Machine		5				
14	Router	Rack mountable router with minimum throughput of 5 Gbps with 2 no's of 10/100/1000Mbps WAN ports and two 1 Gbps LAN ports with static & dynamic routing (OSPF & BGP)	3				
Sub Total (B)							

C. Professional Services for Five Years

Professional Services						
S. No.	**Service**	**Description**	**Unit Rate**	**GST Rate in %**	**First Year Cost Inclusive of GST**	**2nd to 5th Year Cost including GST**
i	Product Setup and implementation	For all the products part of this project scope including production, DR and Test/staging/QA including hardware setup (VM software, network equipment and security devices as recommended)				
ii.	CA Documentation Activities	Support for preparation of CA documentation towards policies & procedures to meet WebTrust compliance requirements - Document readiness review - CP/CPS/PDS creation - BCP/DR documentation - Risk Assessment documentation - Security policies - Register templates				
iii.	Readiness Assessments	For setting up of CA towards Go Live - Infrastructure readiness review including environment, hardware, network, software solutions - CA readiness review with gap assessment of policies, procedures & documentation				
iv.	Compliance Activities	Towards successful compliance of WebTrust - WebTrust audit charges - Support for Internal audits - Support for external audits - Support for resolution of audit findings				
v.	Other Reviews	For any other allied reviews and consultancy in the process of taking CA setup to Go Live				
vi.	Key Generation Ceremony	Support of Key generation ceremony & all the activities there-in				

vii	Operational Training	On-site – 2 business months – Trainers				
viii	Technical Training	On-Site – Senior Consultant (5 days) - based on location				
Sub Total (C)						

D. Manpower Cost for 5 Years

Manpower Requirements		**Costs Inclusive of GST**				
Description	**Nos**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
System Administrator	1					
Network Administrator	1					
PKI Administrator	1					
Security Officer	1					
CA Administrator	1					
Sub Total (D)						

# NIXI reserves the right to change the manpower requirements during the contract period.

Summary of BoM/Commercial Bid

S. No.	**Description**	**First Year Cost Inclusive of GST**	**2nd to 5th Year Cost Including GST**
A	SSL Root Setup Charges		
B	SSL CA Setup Charges		
C	Professional Services Charges		
D	Manpower Costs		
E	Additional Items, if any*		
F	First Year Insurance Charges for all equipments		Not Applicable
TOTAL			

*The bidder must quote item wise details of make, model, configuration and quantities in commercial bid. Details of all additional items, if any (as quoted in reference E in the table above) must also be included into un-priced bill of materials to be submitted in Technical Bid along with their technical specifications & data sheets.

Please Note:

1. The prices are inclusive of GST, all other taxes and include freight, logistics and insurance

costs. GST Values must be mentioned separately for each line item and in totals.

2. Technical & Commercial Evaluation of all bids shall be done based on actual BoM items inclusive of additional items, if any as quoted by the bidder**. Comparison of bids shall be based on the full BoM quantities including additional items, if any as given in this section above**. NIXI retains the right to order as many items as needed out of all quoted items by the bidder.

3. Bidder shall ensure that the solution provided is comprehensive high available for WebTrust requirement and incorporation of CCA root in major Web Browsers.

Delivery Locations:

Sl. No	Location	City Location *
1	Loc 1- Primary	Delhi NCR
2	Loc 2 – Disaster Recovery	Bengaluru

** Address details will be given to successful bidder/ Contractor only.*

Section V: Technical Specifications for the Equipment, Software and Services

A. Technical Requirements:

S. No	Particulars	Score
1*	**SSL Certificate Lifecycle Management Solution (Minimum Specifications)**	**120**
a.	**Platform support**	8
i	**Operation System (OS)**: The proposed solution should be based on either Windows Server 2016 or later version or Linux Operating System with appropriate support of 5 years	1
ii	**Database Server**: The proposed solution should support Enterprise Database Servers with cluster & replication tool bundled to set up primary Data Centre (DC), Disaster Recovery (DR) site with following requirements: • perpetual license with five years OEM Support • database backup with point in time recovery	1
iii	**Virtualization:** It should support virtualization	1
iv	Solution must support LDAP v3 directories for distributing certificates and CRL's.	1
v	A High Availability configuration should be supported with redundancy throughout the server systems.	1
vi	The solution must be properly scalable up to 5 million of certificates	1
vii	There should be a mechanism for monitoring, such as SNMPv3/ Syslog	1
viii	Each component should create operation logs and signed audit logs, error logs with configurable log level and a well-defined syntax.	1
b.	**CA features**	**20**
i	It should support more than one CAs in hierarchy in the same system. The CAs should possibly have different CA policies.	2
ii	It should be possible to assign registration officers to individual CAs or user domains and visibility/ usability of user data should be limited to assigned CA or user domain	2
iii	The CA should be able to publish CRLs and certificates in any number of distribution points using LDAP/HTTPS protocol. The publication address must be configurable for each CA.	2
iv	CRLs should be supported with configurable format, issuing period etc. Mechanism should be in place for publishing revoked certificates on real time basis/ occurrence.	2
v	Support of “immediate” revocation information, i.e., revocation information should be available without latency.	2
vi	The system should support algorithms as such as RSA, ECC and has functions SHA 256 SHA384 and SHA512	2
vii	Support integration with multiple HSMs (over PKCS#11) for storing CA private keys and all other system keys in same instance.	2
viii	Support for satisfactory migration to different CA system before completion of the contract period or discontinuation of contract for whatever reason	6

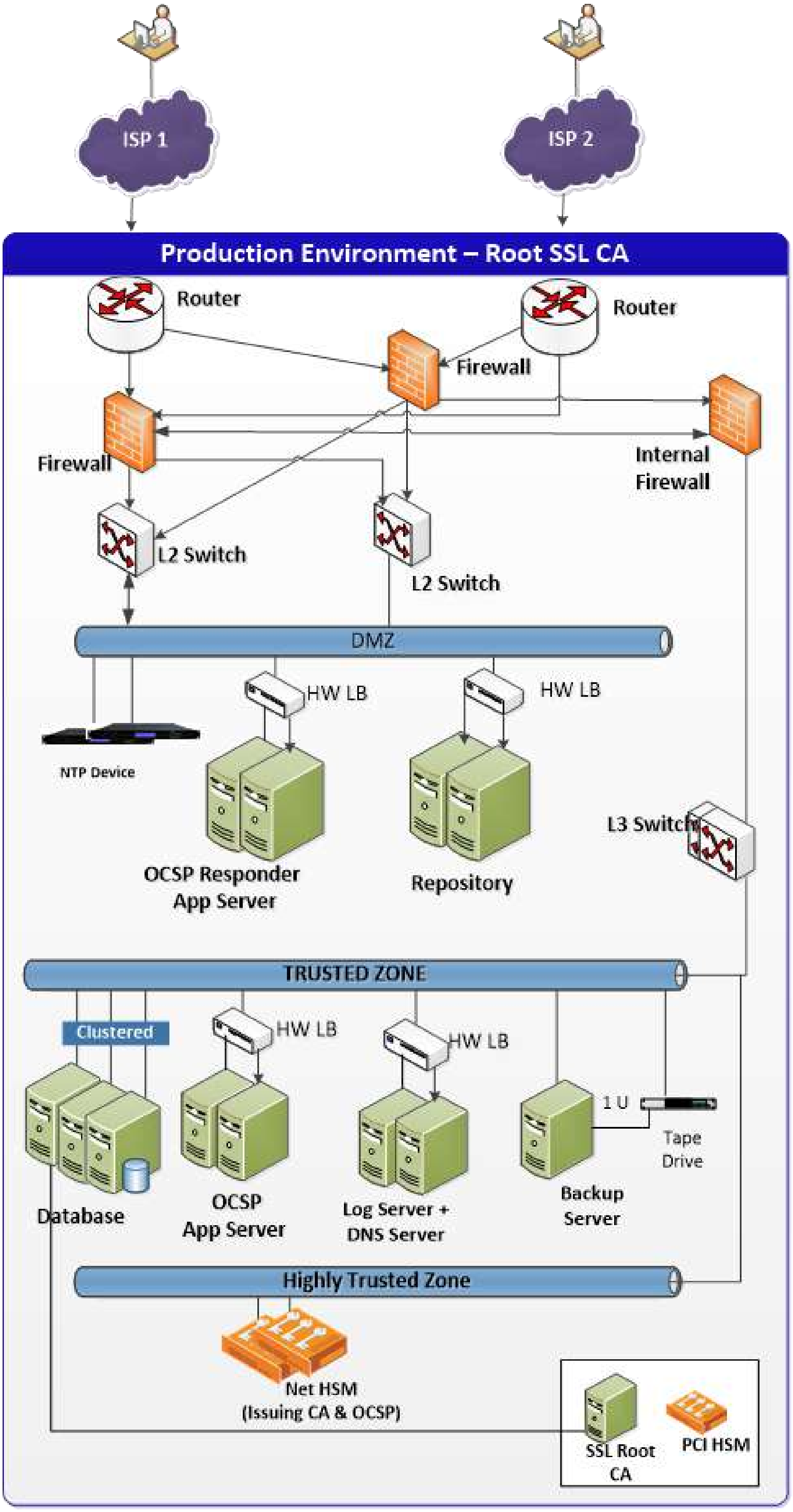
c.	**CA Management**	**12**
i	The product must offer centralized, secure management of CAs, policies and configuration of data with GUI support.	2
ii	It should be possible to manage any number of CAs in any hierarchy in the same system. The CAs should possibly have different CA policies and should be able to define individual policy for each CA.	2
iii	It should be possible to define the CA policies with high granularity: certificate and CRL formats and contents, validity, revocation services (OCSP and/or CRL and/or delta CRL, distribution point address), algorithms.	2
iv	Policies for CA, end entity certificates and CRLs (validity, certificate formats and contents, algorithms etc.) should be defined with high granularity for maximal flexibility.	2
v	Ability to create procedures, policies and profiles in the CA system as per WebTrust requirement	2
vi	Ability to populate values for the certificate's fields and extensions from parameters sent through RA solution or web services as per WebTrust requirement	2
d.	**Certificate Management interfaces**	**4**
	There should be a powerful API that supports certification, revocation for any end entity as well as to retrieve user and certificate information. The API should be access controlled	4
e.	**Administrator Credential Management**	**20**
i	The system must support PKI based authentication for CA solution using Digital Security Certificate (DSC) in USB crypto token.	2
ii	The system must support generating certificates based on PKCS#10 requests.	2
iii	Smart card and token products of leading OEMs/vendor must be supported and lock-in must be prevented by multi card/token support	2
iv	The content of smart cards / tokens and other credential forms should be configurable, e.g. number and purpose of certificates, key length, validity etc.	2
v	Must support the administration of CA via centralized web-based GUI.	2
vi	It should be possible to notify users (managers and end users) about expire of certificates.	2
vii	There should be out of band authentication methods to log into the delegated management system in case of emergency such as card not available, expired, PIN forgotten etc.	2
viii	The input field displayed in Registration Authority client should be configurable	2
ix	CA software should be Common Criteria EAL 4 certified	2
x	CA solution should be WebTrust compliant	2
f.	**Security**	**14**
i	With GUI support, it should be possible to define roles with various permissions (CA management, end entity management, audit, registration, publication, revocation, key recovery, etc.). Access to data and services should be controlled according to the roles.	2
ii	Admin users should be required to authenticate with certificate-based strong two-factor authentication	2
iii	All relevant user actions (e.g., registration, certification, revocation etc.) should be logged in a digitally signed revision safe audit trail (transaction log) which is audit-able.	2

iv	The CA security architecture should have undergone third party penetration testing/ethical hacking tests and proof of audit certificate should be produced	**2**
v	All system credentials should be confidentiality and integrity protected.	2
vi	All system configuration should be integrity protected.	2
vii	All sensitive tasks should require 4-eyes-principle	2
g.	**Scalability and Reliability**	**12**
i	Should support to multiple concurrent HSMs	4
ii	Should support production rate of certificates requests in consistence with HSM capacity.	4
iii	Should support Active - Passive type of high availability ensuring sub components that can be multiplied to match performance and fault tolerance needs.	2
iv	Should allow distributing certificate management services (certificate issuance system, key generation system, CRL generation system, LDAP distribution system and database connecting system) to different physical/logical servers for greater scalability	2
h.	**Interoperability**	**10**
i	Support for all relevant PKIX standards PKCS #1, #5, #7, #8,#9, #10, #11, #12, #15	4
ii	Support for different certificate profiles based on X.509 Public Key Certificates.	4
iii	SDK to customize certificate enrolment, certificate revocation	2
i.	**Interfaces**	**20**
i.	Web Services - Common interface (SOAP) to enable easy integration	5
ii.	SDK - client API with Registration, authorization, all registration functions should be available	5
iii.	Certificate Management Protocol support for both Initial enrollment request and update requests for certificate renewal.	5
iv.	API: Plug-In interface for Registration Authority client	5
2*	**OCSP Specification**	**20**
i	CA shall operate OCSP capability to provide a response time of one second or less under normal operating conditions	5
ii	OCSP responses MUST be signed by an OCSP Responder whose certificate is signed by the CA or its sub-CA that issued the certificate whose revocation status is being checked	5
iii	OCSP request and response messages shall be properly structured and handled according to RFC2560 and RFC6960	5
iv	OCSP Responder can use revocation data from several Certification Authorities (CAs). Multiple instances of responders can be configured to enable separation of different CAs to individual URLs. Alternatively, one responder URL represent all hosted CAs.	5
3*	**Workflow based lifecycle management module Specifications**	**20**
i	The system must be capable of checking expiry of certificates issued and notify the users and administrators accordingly.	10

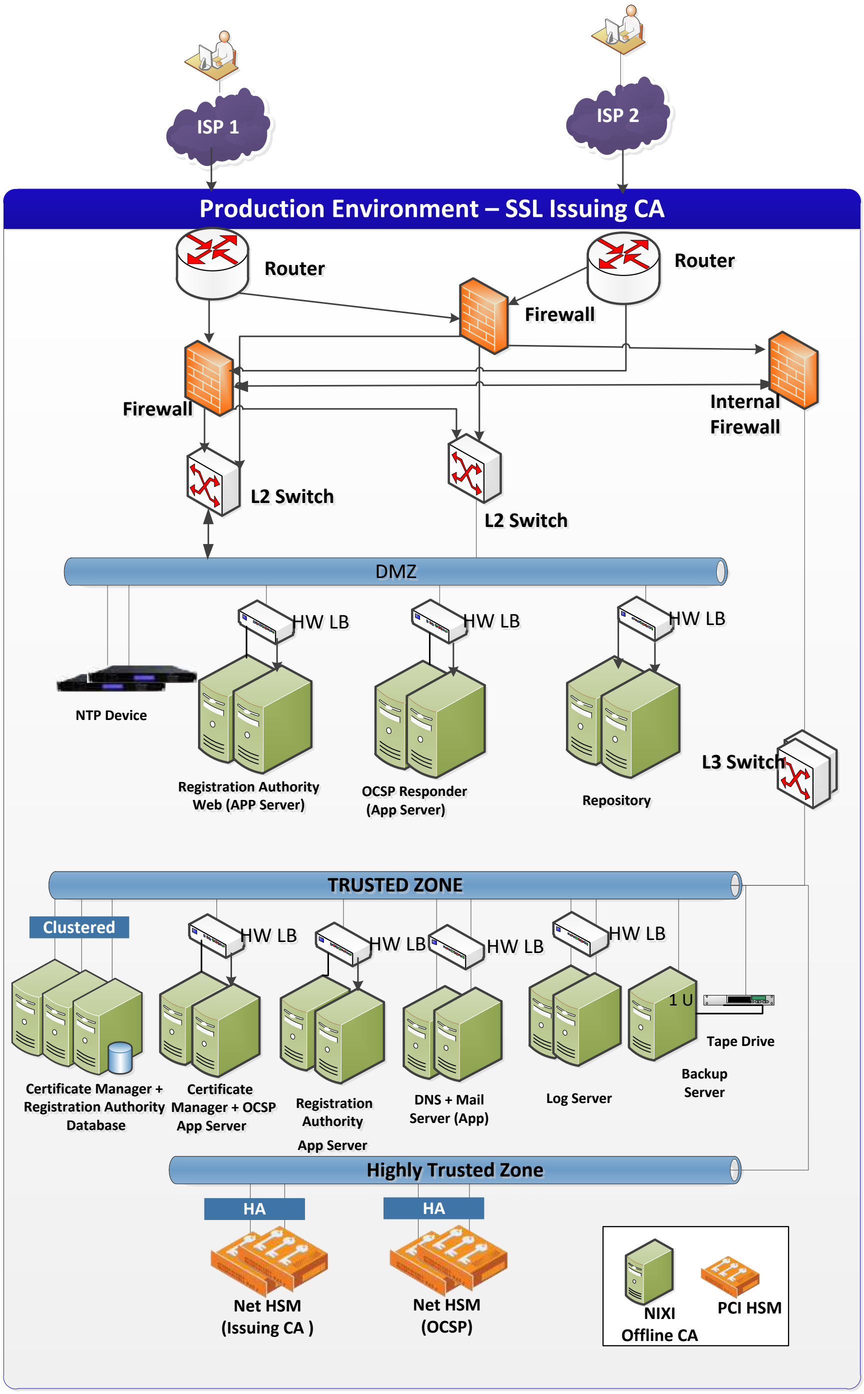
ii	The system must allow administrators to handle user rights and role management.	10
4	**Secure Access**	**10**
i	The proposed solution should have the option to login using multi factor Authentication such as PKI and One Time Passwords to log in as Operator/Administrator.	10
5	**"Compliance to Indian Data Privacy Regulation**	**10**
i	The proposed system should comply with prevailing Indian Data Privacy Regulations.	10

* End of Table *

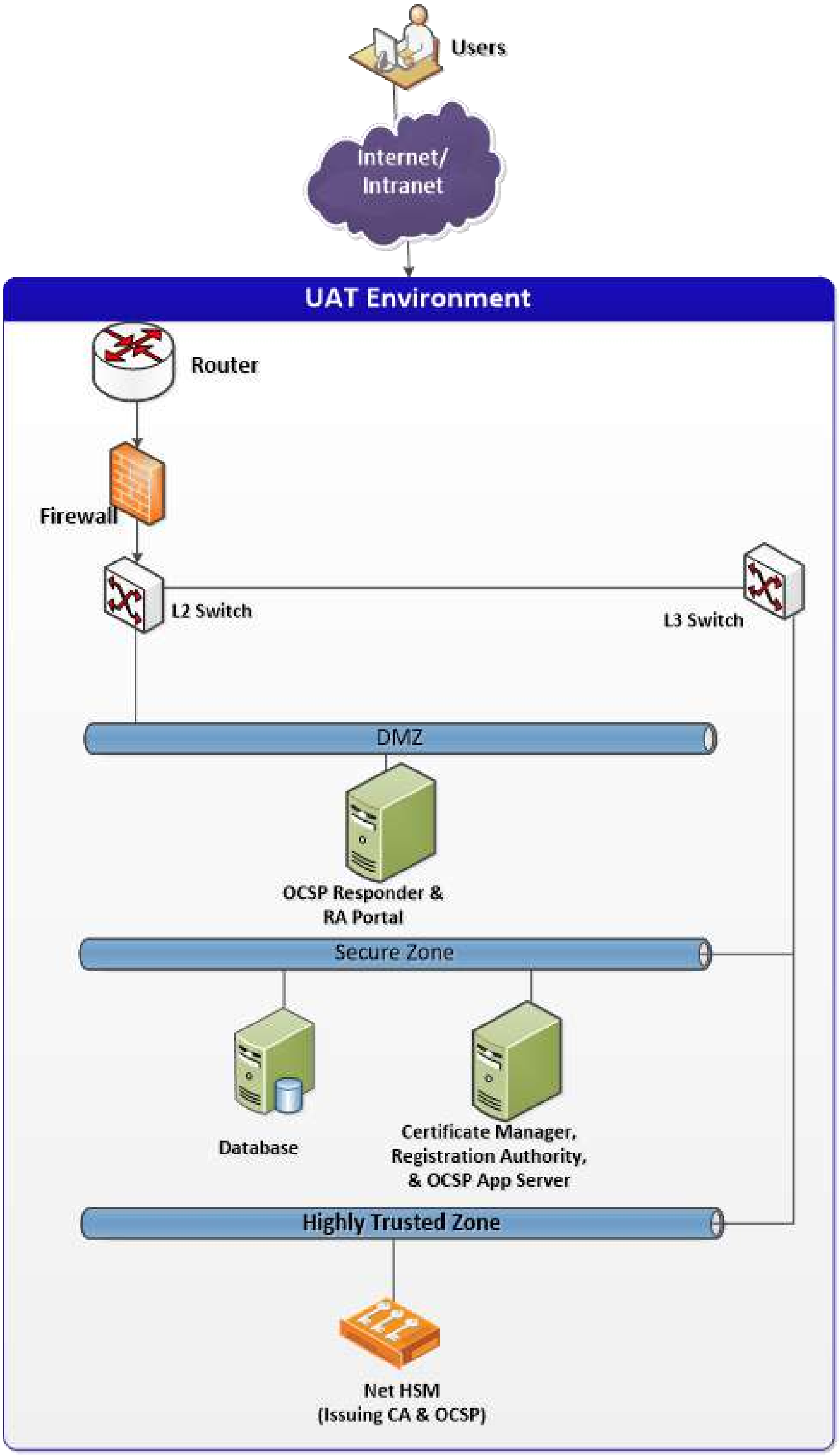
B. Suggested Architecture for Root SSL CA



C. Suggested Architecture for Issuing SSL –CA



D. Suggested Architecture for UAT Environment


Users
Internet/ Intranet
UAT Environment
Router
Firewall
L2 Switch
L3 Switch
DMZ
OCSP Responder & RA Portal
Secure Zone
Database
Certificate Manager, Registration Authority, & OCSP App Server
Highly Trusted Zone
Net HSM (Issuing CA & OCSP)

E. Suggested Specifications:

1. Load Balancer

1	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers. It shall be appliance based and shall facilitate multi-vendor, multi-application environment and shall support third-party products
2	The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit
3	The load balancer shall be built on high-performance hardware, designed for data centres. It shall deliver application traffic of all types and scalable to meet the throughput needs of the most demanding applications. The Load Balancer must ensure high availability for all the services behind the firewall.
4	The Load Balancer shall support offloading of SSL connections
5	The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.
6	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.
7	To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user. The load balancer should support > 3Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software
8	Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Load Balancer shall encrypt or sign these tokens to prevent third party impersonation attacks
	Performance
9	The server load balancer should deliver at least 10 Gbps or higher of layer 7 throughput
10	The server load balancer should deliver > 30 million concurrent sessions
11	The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput on 4096 key
12	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1
13	The sever load balancer should be proposed with 8 Ports populated with 4x1GE, 4x1G SFP ports and aleast 8x10G SFP+ SR ports from day 1
	Features required for Load Balancer
14	Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, Content-based Load Balancing, Persistency, HTTP Content Modifications, QoS, Support for connection pooling to TCP request, Support for distributed denial-of-service (DDoS) protection.
	Load Balancer QoS features
15	It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications
	GSLB
16	It should support load balancing of servers between different data centres without any additional license
	High Availability
17	The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on stateful session failover with Active-active & active standby unit redundancy mode.

2. Firewall:

S. No	Description
1	The appliance-based security platform should be capable of providing firewall, application visibility, IPS and Anti-malware functionality in a single appliance
2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.
	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.
3	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system
4	Console and management ports to access device
5	Appropriate energy efficient redundant (N+N) hot swappable power supplies.
6	Should support Active:Active & Active:Passive modes
	Performance & Scalability
7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)
8	IPS Throughput 5 Gbps
9	Threat Protection Throughput: 5 Gbps
10	Firewall should support at least 8 million concurrent sessions
11	Firewall should support at least 500K sessions per second
12	Firewall should support at least 1000 VLANs
13	Firewall should support at least 8 Gbps of IPSEC VPN throughput
	Firewall Features
14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP
15	Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously
16	Firewall should support operating in routed & transparent mode.
17	Should support Static, RIP, OSPF, OSPFv3 and BGP
18	Firewall should support manual NAT and Auto-NAT, static nat, dynamic NAT, dynamic pa
19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.
20	Firewall solution should support DHCPv6
21	Firewall should support Multicast protocols like IGMP, PIM, etc.
22	Should support security policies based on group names in source or destination fields or both
23	Should support capability to limit bandwidth on basis of apps/groups, Networks / Geo, Ports, etc.
24	Should be supplied with 1000 SSL VPN users license.
25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool

26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.
27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.
28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.
29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.
	High-Availability Features
30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering.
31	Firewall should support ether channel or equivalent functionality for the failover control and providing additional level of redundancy.
32	Firewall should support redundant interfaces to provide interface level redundancy before device failover.
33	Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.
34	Firewall should have integrated redundant power supply.
	Threat Prevention Features/IPS/Anti-Virus
35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.
36	Should be capable of tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
37	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
38	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
39	Should be capable of detecting and blocking IPv6 attacks.
40	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
41	Should must support URL and DNS threat feeds to protect against threats
42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance
43	Proposed solution shall have required subscription like Threat Intelligence for proper functioning.
44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.
45	Should support more than 2000+ application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
46	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).

	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
47	The detection engine should support the capability of detecting variants of known threats, as well as new threats
48	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.
49	Should should have DNS threat intelligence license and feeds to protect against threats
50	Web Application Firewall Protection
51	l Proposed appliance should have in-build WAF with Reverse proxy support,
52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.
53	Server Security.
54	l Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware inspection.
55	l The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console
56	l Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution.
57	Solution must offer vulnerability management to verify servers
	Advance Threat Protection
58	l The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration. Firewall should Identify and control network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create firewall rule lists to block the connection.
	Zero Day threat protection
59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.
60	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.
61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1
62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.
63	Local Malware appliance should have inbuilt feature to send alert over email of detected malware post analysis. For example, if malware has high risk, alert should be notified to security team for further analysis if required.
	Management & Logging/Reporting
64	The management must be accessible via a web-based interface and ideally with no need for additional client software
65	The solution must provide a highly customizable/user friendly dashboard.
66	The solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.

67	The solution must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
68	The management software and log server software must be on two separate virtual machine or two separate dedicated hardware to enable distributed architecture in the environment. The log server should support minimum of usable 5TB storage space in RAID configuration.
69	The solution must provide risk reports like advanced malware, attacks and network
70	Solution must ingest alerts, enrich and orchestrate with visual playbooks editor for automatic response.
71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.
72	The solution must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.
73	Certification
74	Operating system of NGFW solution must support: USGv6 / IPv6, FIPS-140-2 / Common criteria EAL4/ICSA.

3. Tape Drive:

Available configuration	Fibre Channel Drives F9C & F95 and SAS Drives S9C – One LTO Ultrium 9 full height internal tape drive
Interface	12 Gb SAS or 8 Gb FC
Tape drive type	LTO Ultrium 9
Physical capacity	18 TB native; 45 TB with 2.5:1 Compression
Number of tape drives	1
Number of tape cartridges	1
Data transfer rate	Up to 400 MBps native SAS and 700 MBps FC with 2.5:1 compression
Media Type	Read and Write LTO Ultrium 9 • 18 TB data cartridge • 18 TB WORM cartridge LTO Ultrium 8 • 12 TB data cartridge • 12 TB WORM cartridge LTO Ultrium cleaning cartridge
Power Requirements	100 – 240 V ac.50 – 60 Hz auto-ranging
Dimensions	19inch rack mountable

4. HSM Module:

S.No	Minimum Technical Specification
1	HSM should be network based appliance with inbuilt NIC support for 1 GB and 10 GB network .
2	Support for operating systems like Windows & Linux

3	Virtual System support like VMware, Hyper-V etc
4	Host Interface: Should have inbuilt Dual Gigabit Ethernet ports with port bonding and Dual 10G network port with port bonding. All four NICs should have IPv4 and IPv6 support. Capabilities should be from day 1
5	Cryptographic APIs: PKCS#11, Java /JCE, Microsoft CAPI and CNG, Open SSL
6	Cryptography: Full CSNA suite support
7	Asymmetric: Support for various cryptographic algorithms: CSNA suite support , Asymmetric Key RSA (512-4096 bits), DSA , ECDSA , ECDH, Ed25519, ECIES, ECC (No separate license of Algorithm to be charged)
8	Symmetric: AES, Triple DES, DES (No separate license of Algorithm to be charged).
9	Support for Hash Message Digest HMAC, SHA1, SHA2 (512), SM3 and SM4
10	Key Derivation and Key Wrapping support
11	HSM should be FIPS 140-2 Level 3 certified and certification should be in OEM Name. Certification Copy needs to be submitted
12	HSM should have GUI capabilities for , crypto management , backup/restore management ,user management , & HSM upgrade management without need of customer to build any software/interface from HSM APIs.
13	HSM should have simulator capabilities to provide development , integration and Testing of applications in restricted network with no outside connectivity to internet .
14	Clustering, Load Balancing should be supported
15	Ability to generate RSA & ECC keys (2048 to 4096 or equivalent) . Support for ECC curve NIST P-256,P-384 or P-521 at no cost
16	Keys always secured by FIPS-validated, tamper-evident hardware. Ability to generate RSA keys (2048 to 4096) on board on demand. All Keys must be secured and protected using FIPS 140-2 level 3 certified HSM
17	Multiple roles for strong separation of duties
18	Secure audit logging
19	The proposed solution should be in High Availability in DC and DR for redundancy, reliability and disaster recovery
20	HSM should have multifactor authentication using tokens/smart card for enhanced Security Support.
21	Minimum Performance: RSA-2048: 500 TPS
22	HSM should have capabilities to increase TPS on same appliance by applying license or upgrade package . In case of Hardware replacement or addition of new appliance to increase the TPS , Cost of additional hardware should be included by HSM OEM in BOM during initial stage as per organization's guidelines. OEM must provide Doom’s Day service whenever needed by client at no additional cost
23	Should Support MTBF 100000 Hrs or More
24	Provide new version upgrades, updates, patches, etc for all the components/ sub-components through the period of contract. 24/7 telephonic and email OEM support. OEM should be present in India and one PO should be furnished for same. OEM should have warehouse in India of its own or from distributor/partner
25	The required solution must not be End of Life or End of Support for at least 5 years from the due date of submission of bid by the bidder
26	HSM should have unlimited client Licenses (Should not have separate cost of any client License)

5. PCIe HSM Specifications

Operating Systems	Support for Microsoft Windows 2016 or higher
Physical Characteristics	Should Support PCIe with external smart card reader
Host Connectivity	PCIe x4
Application Program Interfaces (APIs)	PKCS#11, Java (JCE), Microsoft CAPI
Key backup	Support for key backup in external storage media in encrypted form
Support Availability in India	Support should be available in New Delhi and Bangalore
Cryptography	Asymmetric public key algorithms: RSA (2048, 4096 or higher) with ECC (NIST P-256, P-384 & P-521)support
Hash/message digest:	SHA-2 (224, 256, 384, 512bit)
Safety , Security and Environmental Compliance	FIPS 140-3 Level 3, NIST SP 800-131A with valid certification
End of life	Should not be less than 5 years from date of P.O
Power	Should be suitable for offline environment(no power supply for longer period). No failure due to prolonged absence of power supply to HSM PCIe devices

6. Layer 3 Switch

Sl. No.		DESCRIPTION
1	General Requirements	L2 Managed Switch should have minimum 24x GE RJ45 and 4x 10GE SFP+ and dedicated ports atleast 2x40G ports to connect the Fiber uplink it should support SX, LX and copper transceivers
2		The proposed switch form factor should 1 RU Rack-Mount Appliance and Should have one RJ-45 Serial console port
3		Switching capacity of the proposed switch should be minimum 288 Gbps and 428 Mpps Packet per second.
4		Proposed Switch should support minimum 32K MAC address storage and 4000 VLAN's
5		The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat
6		Switch should support AC built in with Redundant Power
7		Should support min DRAM 2GB and 128MB of Flash, maximum to be specified
8	Layer 2, Layer 3 &	Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root Guard

9	Authentication Requirements	Switch should support DHCP snooping IPv4 / IPv6, IP source guard, IP source-guard violation log, Dynamic ARP inspectio, IPv6 RA guard, IGMP snooping/proxy/querier, VLAN stacking (QnQ) , MCLAG, QoS marking (IPv4/IPv6), Should have management protocol that allows NGFW Security Appliance to seamlessly manage any Ethernet Switch
10		Should support IEEE 802.1AX Link Aggregation, IEEE 802.1q VLAN tagging, LLDP/MED
11		Switch should prevent direct client-to-client traffic visibility at the layer-2 VLAN.
12		Should support 802.1x port-based authentication
13		Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB)
14		Should support IEEE 802.1x Guest and Fallback VLAN
15		Should support IEEE 802.1x Dynamic VLAN Assignment
16		Switch should support local user database and can integrate with RADIUS, Radius CoA,TACACS+ servers
17		Switch should support IPv4 16K Route Entries and 8K Ipv6 Route Entries
18		Switch should support 1K ACL count. It should also support Dynamic ACL
19		Switch should support Static routing (IPv4/IPv6) , Hardware-based routing (IPv4/IPv6), DHCP server and relay
20		Switch should support Layer 3 Policy-based routing, OSPF (IPv4/IPv6), BFD for OSPF (IPv4/IPv6), RIP (IPv4/IPv6), BFD for RIP (IPv4/IPv6) ,VRRP (IPv4/IPv6), BGP (IPv4/IPv6) , IS-IS (IPv4/IPv6) , BFD for IS-IS (IPv4/IPv6)
21	Management	Should support SSH, HTTP,HTTPS with IPv4 and IPv6 Management
22		Switch should support SNMP v1, v2c and v3
23		Proposed switch should be managed via both, GUI and CLI
24		Switches must be ready for centralized management from day one with the below key features to support. Bidder should provide all the required hardware and software resources and licenses from day one to achieve the below management features.
25		Switch should be ready from day one to offer visibility, user access control, and threat mitigation at the switch port level.
26		Switch should discover automatically by centralized management and configures with Zero-touch provisioning
27		Should support centralized management : configuration and reporting, Software Upgrades of Switches through a single console
28		Should have option to create switch profiles to allow specific settings to be applied to all authorized Switches.
29		Centralized management should show the network topology of all managed switches through a single console
30		Central management solution should have Robust Monitoring – Topology views of all managed switches, Port level view, Status monitoring views from single console.

31		Switch must have option to ping using Switch serial number instead of the Switch IP address.
32		Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN. And Based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. If bidder not supported in-built they should include all the required hardware and software resources.
33		Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN.
34		Bidder should inlcude all the required components and licenses to achieve all the specified specifications.
35	Environment	Power Required :100–240V AC, 50–60 Hz
36		Operating Temperature : 0–45°C, Storage temperature: -40–70°C, Humidity: 5–95% non-condensing
37	Certification	FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2

7. Server

S. No.	Parameter	Specifications
i.	Processor	Processor with 2.4 Ghz and above (Intel/AMD)
ii.	No of cores	16
iii.	No of Processors	2
iv.	Chipset	Intel /AMD updated version
v.	Memory	256 GB using 8x32GB DIMM’s Only, PC3-12800R (DDR4-3200 Mhz) or higher Registered DIMMS Shall be expandable upto 768GB or higher"
vi.	PCI Slots	Minimum 2 nos. of PCI-Express Gen4 Slot shall be available for future expansion (After taking into account all the mandatory and optional hardware mentioned in this document)
vii.	HSM Module	Should support PCIe based HSMs

viii.	Interface Ports	a) Serial port - 1;
		b) Mouse - 1;
		c) Keyboard - 1;
		d) VGA Graphics - 1;
		e) USB 3.0 or above - 4;
		f) RJ45 Network ports - 4 +1(for Remote
		e) FC Network Port (10 G) – 2* 2x10 G
		Management)
		(In case Mouse and Keyboard are USB based then additional USB ports to be given. Similarly for serial port converted from USB, additional USB port shall be provided along with USB to Serial converter.)

ix.	Hard Disk Drive	Enterprise SSD with 3 * 2 TB
x.	Bays	Should support minimum 6 nos. of SSD Drives
xi.	RAID Controller	6 Gbps or higher throughput HW RAID Controller supporting RAID 0/1/1+0/5/6 with minimum **1 GB** of Flash-backed write cache.
xii.	FC HBA	2 x single Port Qlogic 16 Gbps FC Host Bus Adapter
xiii.	Optical Drive (internal)	DVD-ROM Drive(or DVD/CD Compatible Blu-Ray Disc Drive)- Optional
xiv.	Graphics Controller	Integrated on-board graphics with support for 16 Million color: resolution of 1280 x 1024
xv.	Gigabit Ethernet ports	4 nos of Gigabit Ethernet ports full duplex. The network ports should also provide the following functionalities for all supported OS: · Ethernet Bonding, Failover and load balancing, · Wake on LAN, · Pre-Boot Execution Environment (PXE), · Multiple VLAN tagging, · Auto-negotiation for 10/100/1000 Mbps
xvi.	Redundant Power Supplies	Redundant Hot Plug Power Supplies (230 VAC) The power supplies shall be either 80 Plus gold certified or better
xvii.	Redundant cooling Fans	Redundant Hot Plug fans
xviii.	Form Factor	Rack mountable with rack mount kit and rails (preferably 2U or less)
xix.	OS Support	The quoted server should support the following Operating Systems: a) Microsoft Windows Enterprise Server 2016 R2 and above; b) RHEL 7 and above ; c) Vmware vSphere™ 7.0 and above d) Ubuntu / CentOS updated Version

xx.	Remote Manageability	a) It shall be possible to manage the server hardware and software components remotely. b) The server hardware shall be manageable even when it is shutdown or crashed. c) Drivers for automatic fencing shall be provided for RHEL. d) It shall be possible to power on/off and boot the system remotely; e) It shall have the following features: · real time power reading; · POST and failure sequence replay; · Event log; · Browser and CLI support; · Secure Socket Layer; · Secure Shell.
xxi.	Server Management	OEM software for management of Servers must be included as standard. It should integrate with any SNMP based industry standard Network Management Software. (The SNMP MIBs for all the hardware and software components shall be provided in a DVD media). Should provide Fault management and automatic event handling through e-mail, SMS. Should provide Role based secured remote management using Secure Sockets Layer (SSL) and Secure Shell (SSH) to encrypt management communications. Should provide pre-failure warning for CPU, Memory & HDD. Should have local LED/LCD based diagnostic panel for easy fault identification.

Please Note:

The specifications mentioned are the minimum suggested ones, Bidders will ensure that the items quoted meet WebTrust and all tender’s requirement and they are welcome to quote equipment/Software/Hardware which have higher (more) specifications than as mentioned above.

Section VI: Qualification Criteria

1. As defined in NIT clause 3, Bidder must meet all the eligibility and experience criteria.

2. Copy of Board Resolution and/ or Power of attorney on Stamp Paper for authorize signatory which authorizes the signatory to commit and submit bids on behalf of the bidder shall be submitted along with technical proposal. Failing of which the bid will liable to be rejected.

3. In case, Bidder is Startup then such Bidder must have completed at least one project of establishing the WebTrust compliant SSL CA facility along with incorporation of SSL root in Major Web browsers.

4. Bidder shall provide supporting document(s) viz. the customer purchase orders, scope of work, deliverables, project value and satisfactory work completion certificate from client(s). Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder.

5. The bidder must be an authorized representative of the products offered. The Manufacturer authorisation form (MAF) from the OEM must be submitted along with the bid. Authorisation must be issued by OEM's authorise signatory. OEMs MAF should contain the following points in its MAF while issuing to bidder:

   a) Offered equipment (s) should not be declared end of life/support for next five years.
   b) Offered equipment (s) should not be declared end of sale before installation.
   c) Make and Model of Offered equipment(s).
   d) Equipment supplied by the OEM should be transferrable to any other government agency at a later date along with warranty and support commitments.

6. Bidder should have required infrastructure for onsite service support. *Relevant details to be submitted with Bid Document.*

7. **Malicious Code Certificate:**
   Bidder should upload following certificate in the bid:
   a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:
   i. Inhibit the desires and designed function of the equipment.
   ii. Cause physical damage to the user or equipment during the exploitation.
   iii. Tap information resident or transient in the equipment/network.
   b) The bidder/entity will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

8. OEMs shall not be debarred/blacklisted/suspended by Government. *A self-declaration to this effect from respective OEMs shall be required to be submitted by the bidder at the time of submission of bid.*

9. The Make & model of the IT equipment offered in bid should be listed (along with Data Sheet) on the OEM website. *Relevant details shall be submitted with bid.*

BIDDING FORMS

Form 1: Bid Form (Covering Letter)

(To be submitted as part of Technical bid, along with supporting documents)

(On Bidder's Letter-head)

To

CEO, National Internet Exchange of India (NIXI),
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road, New Delhi 110001

Sir,

Having examined the abovementioned Tender Document, we, the undersigned, hereby submit our Technical and Financial bid (Price Schedule) for the supply of Equipment and all Works/ Services in conformity with the said Tender Documents.

(Please tick appropriate boxes or strike out sentences/ phrases not applicable to you)

1) Our Credentials:

We are submitting this bid on our behalf, registered in India under the Indian Companies Act 1956/2013 as amended Our company law and taxation regulatory requirements and authorization for signatories and related documents are submitted in Form 1.1 (Bidder Information).

2) Our Eligibility and Qualifications to participate

We comply with all the eligibility criteria stipulated in this Tender Document, and the relevant declarations are made along with documents in Form 1.2 of this bid-form. We fully meet the qualification criteria stipulated in this Tender Document, and the relevant details are submitted along with documents in Form 4: 'Qualification Criteria - Compliance.

3) Our Bid to supply of Equipment & Services:

We offer to supply the subject Equipment of requisite specification and within Delivery Schedules in conformity with the Tender Document. The relevant details are submitted in Form 2: 'Bill of Material - Compliance and Form3: 'Technical Specifications - Compliance.'

4) Prices:

We hereby offer to perform the Services at our lowest prices. The prices in this offer have been arrived at independently, without restricting competition, any consultation, communication, or agreement with any other bidder or competitor relating to:

i) those prices; or
ii) the intention to submit an offer; or
iii) the methods or factors used to calculate the prices offered.

The prices in this offer have neither been nor shall be knowingly disclosed by us, directly or indirectly, to any other bidder or competitor before bid opening or contract award unless otherwise required by law.

5) Affirmation to terms and conditions of the Tender Document:

We have understood the complete terms and conditions of the Tender Document. We accept and comply with these terms and conditions without reservations and deviations.

6) Bid Securing Declaration

We have submitted the Bid Securing Declaration (BSD, in lieu of Bid Security) in stipulated format vide Form 7: ‘Documents Relating to bid security.’

7) Abiding by the Bid Validity

We agree to keep our bid valid for acceptance for a period upto 75 days from bid submission, as required in the Tender Document or fora subsequently extended period, if any, agreed to by us and are aware of penalties in this regard stipulated in the Tender Document in case we fail to do so.

8) Non-tempering of Downloaded Tender Document and Submitted Scanned Copies

We confirm that we have not changed/ edited the contents of the downloaded Tender Document. We realize that any such change noticed at any stage, including after the contract award, shall be liable to punitive action in this regard stipulated in the Tender Document. We also confirm that scanned copies of documents/ affidavits/ undertakings submitted along with our Technical bid are valid, true, and correct to the best of our knowledge and belief. If any dispute arises related to the validity and truthfulness of such documents/ affidavits/ undertakings, we shall be responsible for the same. Upon accepting our Financial bid, we undertake to submit for scrutiny, on- demand by the NIXI, originals, and self-certified copies of all such certificates, documents, affidavits/ undertakings.

9) A Binding Contract:

We further confirm that, if our bid is accepted, all such terms and conditions shall continue to be acceptable and applicable to the resultant contract, even though some of these documents may not be included in the contract Documents submitted by us. We do hereby undertake that, until a formal contract is signed or issued, this bid, together with your P.O shall constitute a binding contract between us.

10) Performance Guarantee and Signing the contract

We further confirm that, if our bid is accepted, we shall provide you with performance security of the required amount stipulated in the Tender Document for the due performance of the contract. We are fully aware that in the event of our failure to deposit the required security amount and/ or failure to execute the agreement, the NIXI has the right to avail any or all punitive actions laid down in this regard, stipulated in the Tender Document.

11) Signatories:

We confirm that we are duly authorized to submit this bid and make commitments on behalf of the Bidder. Supporting documents are submitted in Form 1.1 annexed herewith. We acknowledge that our digital/digitized signature is valid and legally binding.

12) Rights of the NIXI to Reject bid(s):

We further understand that you are not bound to accept the lowest or any bid you may receive against your above-referred Tender Document.

……………………..

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of

[name & address of Bidder and seal of company]

Form 1.1: Bidder Information

(To be submitted as part of Technical bid along with supporting Documents)

(On Company Letter-head)

(Along with supporting documents, if any)

Bidder's Name_________________[Address and Contact Details]

Bidder's Reference No.__________________

Tender Document No. Tender No./ xxxx

Note: Bidder shall fill in this Form following the instructions indicated below. No alterations to its format shall be permitted, and no substitutions shall be accepted. Bidder shall enclose certified copies of the documentary proof/ evidence to substantiate the corresponding statement wherever necessary and applicable. Bids shall be liable to be rejected as nonresponsive if Bidder's submits any wrong or misleading information and NIXI may invoke Bid Security Declaration.

(Please tick appropriate boxes or strike out sentences/ phrases not applicable to you)

1) Bidder/ Contractor particulars:

a) Name of the Company: ………….
b) Corporate Identity No. (CIN): ……………………………………..
c) NIXI Supplier ID ……………………………
d) Place of Registration ………………….
e) Complete Postal Address: …………………………………………..
f) Pin code: ………………………………………………….
g) Telephone nos.: ……………………
h) Mobile Nos.: ……………………..
i) Contact persons/ Designation: …………………………………….
j) Email IDs: ………………………………………………………….

Submit documents to demonstrate eligibility as per NIT-Clause 3- Certificate of incorporation/Registration attested by Company Secretary/ Authorized Signatory

2) Taxation Registrations:

a) PAN number: ……………………………………………….
b) Type of GST Registration as per the Act (Normal Taxpayer, Composition, Casual Taxable Person, SEZ, etc.): ………………………….
c) GSTIN number: …………………………………….
d) We solemnly declare that our GST rating on the GST portal/ Govt. official website is not negative/ blacklisted.

Documents to be submitted: Self-attested Copies of PAN card and GSTIN Registration.

3) Authorization of Person(s) signing the bid on behalf of the Bidder

a) Full Name: ____________________
b) Designation: ______________________
c) Signing as:

□ A company. The person signing the bid is the constituted attorney by a resolution passed by the Board of Directors or Power of attorney given on stamp paper by authorize person.

Documents to be submitted: Power of Attorney/ Board Resolution

4) Bidder's Authorized Representative Information

a) Name:
b) Address:
c) Telephone/ Mobile numbers:
d) Email Address:

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form1.2: Eligibility Declarations

(To be submitted as part of Technical bid)

(On Company Letter-head) (Along with supporting documents, if any)

Tender Document No. Tender No./ xxxx;

Bidder's Name_________________[Address and Contact Details]

Bidder's Reference No.__________________

Note: The list below is indicative only. You may attach more documents as required to confirm your eligibility criteria.

Eligibility Declarations

(Please tick appropriate boxes or cross out any declaration not applicable to the Bidder)

We hereby confirm that we are complying with all the stipulation of NIT-clause 3 and ITB-clause 4.1.2 and declare as understand shall provide evidence of our continued eligibility to the NIXI as may be requested:

1) Legal Entity of Bidder: ________________

We solemnly declare that we (including our affiliates or subsidiaries or constituents):

a) are not insolvent, in receivership, bankrupt or being wound up, not have our affairs administered by a court or a judicial officer, not have our business activities suspended and are not the subject of legal proceedings for any of these reasons;

b) (including our Contractors/ subcontractors for any part of the contract):

i. Do not stand declared ineligible/ blacklisted/ banned/ debarred by Government from participation in its Tender Processes; and/ or

ii. Are not convicted (within three years preceding the last date of bid submission) or stand declared ineligible/ suspended/ blacklisted/ banned/ debarred by appropriate agencies of Government of India from participation in Tender Processes of all of its entities, for offences mentioned in Tender Document in this regard. We have neither changed our name nor created a new "Allied Firm", consequent to the above disqualifications.

c) We certify that we fulfil any other additional eligibility condition if prescribed in Tender Document.

d) We have no conflict of interest, which substantially affects fair competition. The prices quoted are competitive and without adopting any unfair/ unethical/ anti-competitive means. No attempt has been made or shall be made by us to induce any other bidder to submit or not to submit an offer to restrict competition.

e) We have gone through F.No.6/18/2019 – PPD dated 23rd July 2020 issued by Department of Public Procurement, Ministry of Finance, Govt. of India and certify as follows:

I hereby certify that the <<<<bidder’s name>>>> :

(i) is not from such a country

or

(ii) is from such a country and has been registered with the Competent Authority in India which makes the bidder eligible to participate in this RFP. [Evidence of valid registration by the Competent Authority attached.]

I hereby certify that <<<<<<bidder name>>> fulfils all requirements in this regard and is eligible to be considered.
{Strike out inapplicable clause i.e. clause (i) or (ii)}

2) Make in India Status:

Having read and understood the Public Procurement (Preference to Make in India PPP - MII) Order, 2017 (as amended and revised till date) and related notifications from the relevant Nodal Ministry/ Department, and solemnly declare the following:

a) Self-Certification for the category of suppliers:

(Provide a certificate from statutory auditors/ cost accountant in case of Tenders above Rs 10 Crore for Class-I or Class-II Local Suppliers). Details of local content and location(s) at which value addition is made are as follows:

Local Content and %age	
Location(s) of value addition	

Therefore, we certify that we qualify for the following category of the supplier (tick the appropriate category):

□ Class-I Local Supplier/

□ Class-II Local Supplier/

□ Non-Local Supplier.

b) We also declare that.

□ There is no country whose bidders have been notified as ineligible on a reciprocal basis under this order for the offered Services, or

□ We do not belong to any Country whose bidders are notified as ineligible on a reciprocal basis under this order for the offered Services.

MSME Status:

Having read and understood the Public Procurement Policy for Micro and Small

Enterprises (MSEs) Order, 2012 (as amended and revised till date), and solemnly declare the following:

a) We are - Micro/ Small/ Medium Enterprise: ……………..

b) We attach herewith, Udhyam Registration Certificate with the Udhyam Registration Number as proof of our being MSE registered on the Udhyam Registration Portal. The certificate is the latest up to the deadline for submission of the bid.

c) Whether Proprietor/ Partner belongs to SC/ ST or Women category. (Please specify names and percentage of shares held by SC/ ST Partners): …………….

Penalties for false or misleading declarations:

We hereby confirm that the particulars given above are factually correct and nothing is concealed and undertake to advise any future changes to the above details. We understand that NIXI may invoke Bid Security Declaration, if any wrong or misleading self-declaration submitted by us.

……………………..

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of

…………………………

…………….

Dated…………………

……..

Place……………………………………

[name & address of Bidder and seal of company]

Form 1.3: OEM's Authorization

CEO, NIXI
Statements House Building, 9th Floor
Barakhamba Road, New Delhi-110001

Sub: Manufacture Authorization for (MAF) to M/s < Name of Bidder>

Ref: Tender No.:

This is to certify that the bidder M/s______________________________(name of bidder) is representing us, M/s__________________________________(name of OEM) for____ (name of product category) for the above referred tender no.

We confirm that we have understood the delivery& installation timelines defined in the tender. We confirm that we have worked out all necessary logistics and pricing agreement with <<<Bidder Name>>> and there won't be any delay in delivery, installation and support due to any delay from our side. Our full support is extended in all respects for supply, warranty and maintenance of our products. We undertake that offered product/software in this bid are not obsolete and will not be declared end of life for next 5 (five) years beginning from the date of successful installation & acceptance and also assure that the support including spares, patches, upgrades, updates, etc. for the quoted products/software shall be available for next 5 (five) years.

In case of any difficulties in logging complaint at bidder end, NIXI will have option to directly log complaints at our call support center. We ensure that our offered equipment's are IPv6 ready from day one.

We undertake that equipment supplied by the OEM should be transferrable to any other government agency at a later date along with warranty and support.

M/s__________________________(name of OEM) hereby certify that the products offered for this tender are not declared end of sale and if any of the product is declared end of sale during the installation and commissioning phase, it will be replaced with suitable equivalent or higher rollover product.

We also undertake that in case of default in execution of this tender by < name of bidder>, M/s <name of OEM> will provide necessary support to NIXI in identifying another partner with similar certifications/capabilities and extend support to the new partner in line of this bid. Our details are as under:

Name of the Company: ……………………………………………….

Complete Postal Address: …………………………………………. ..

Pin code: ……………………………………………….

Telephone nos.: ………………………….

Fax No.: …………………………………

Mobile Nos.: ……………………………

Contact persons/ Designation: ……………………………………….

Email IDs: ……………………………………………………………….

The warranty shall be onsite replaceable warranty of the products that are listed below. I also certify that the below mentioned product being supplied by the <Name of Bidder> meets the minimum specifications given in the bid.

Sl. No.	Name of Equipment	Make & Model	Remarks (if any)

Yours faithfully,
Name & Designation of Authorize Signatory:
Signature & Seal:
Date:
Place:

[name & address of Authorize Signatory and seal of company]

Form 2: Bill of Material - Compliance

(on Company Official Letter Head)

Bidder's Name_________________

[Address and Contact Details]

Bidder's Reference No.___________

To

CEO, National Internet Exchange of India (NIXI),
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road, New Delhi 110001

Date………

Ref: Tender Document No. Tender No./ xxxx;
Subject: Bill of Material (BoM) Compliance

There are no deviations (null deviations) in Bill of Material mention in Section IV in Tender Document. <<M/s Bidder's Name ->> certify that our proposal includes all the equipment & services specified in tender document.

We understand that the requirement of equipment(s) & services briefed in **Section-IV- Bill of Material**; we confirm that we have undertaken our own assessment for complete implementation of project and accordingly we have considered extra Equipment, software, application and services etc. (if any) will be provided by << M/s Bidder's Name >>>> to complete the project without any additional costs to NIXI.

"This is to certify that our proposed bid includes all the Equipment and service mentioned in **Section-IV-Bill of Material** as well as other material or service based on self-assessment to complete the project and meets all the requirements of the tender document including but not limited to Scope of Work (including SLAs), Business Requirements and Functional Specifications/ Requirements.

In case, any equipment or software or services is found non-compliant at any stage during project implementation or after acceptance, it would be replaced with a fully compliant product/ solution at no additional cost to NIXI. In case of non-adherence of this activity, NIXI reserves the right to cancel the contract, in case the said Contract is awarded to us by NIXI.

We shall comply with Warranty & Support requirements in the Tender Document.

We further confirm that our technical and financial bid is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work

Yours faithfully, (Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form3: Technical Specifications- Compliance

(on Company Official Letter Head)

Bidder's Name________________

[Address and Contact Details]

Bidder's Reference No.________________

To

CEO, National Internet Exchange of India (NIXI),
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road, New Delhi 110001
Ref: Tender Document No. Tender No./ xxxx;

Subject: **Section V- Technical Specification Compliance**

There are no deviations (null deviations) in Technical Specification mention in **Section V- Technical Specification** in Tender Document. <<M/s -------------------->> certify that our proposal fulfil specification of each Equipment & Service specified in tender document.

We understand that the Specification of equipment(s) & services briefed in **Section V- Technical Specification**; we certify that our proposed equipment(s) & services are same or higher than the minimum technical specifications as given in the tender document.

In case, any equipment or software or services is found non-compliant at any stage during project implementation or after acceptance, it would be replaced with a fully compliant product/ solution at no additional cost to NIXI. In case of non-adherence of this activity, NIXI reserves the right to cancel the contract, in case the said Contract is awarded to us by NIXI.

We further confirm that our commercial proposal is for the entire scope of work, comprising all

required components, specifications and our obligations, for meeting the scope of work.

Enclosure:- Compliance Statement of Section- V and required and relevant documents like technical data, literature, drawings, datasheets, test Reports/ Certificates and or/ or Type Test Certificates (if applicable/ necessary) with supporting documents, to establish that the Equipment and Services offered in the bid fully conform to the Equipment and Services specified by the NIXI in the Tender Document along with this compliance.

……………………..

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of

[name & address of Bidder and seal of company]

Form 4: Qualification Criteria - Compliance

(on Company Official Letter Head)

Bidder’s Name__________________

[Address and Contact Details]

Bidder’s Reference No.___________________

To

CEO, National Internet Exchange of India (NIXI),

9th Floor, B-Wing, Statesman House,148, Barakhamba Road, New Delhi 110001

Ref: Tender Document No. Tender No./ xxxx;

Subject: **Section-VI- Qualification Criteria - Compliance**

Note to Bidders: Furnish statements and documents to confirm conformity to Qualification Criteria may be mentioned/ attached here. You may attach documents as required for qualification criteria. Add additional details not covered elsewhere in your bid in this regard. Non-submission or incomplete submission of documents may lead to rejection of the bid as nonresponsive.

Documents Attached supporting the compliance to qualification criteria in Section-VI:

Sl. No.	**Document Attached, duly filled, signed, and copies self-attested**
1	
2	
3	
..	

Yours faithfully, (Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form4.1: Experience Statement

Statement of completion of Project Last five Years

(on Company Official Letter Head)

Bidder's Name________________

[Address and Contact Details]

Bidder's Reference No.__________________

To

CEO, National Internet Exchange of India (NIXI),

9th Floor, B-Wing, Statesman House,148, Barakhamba Road, New Delhi 110001

Ref: Tender Document No. Tender No./ xxxx;

Subject: **Section-VI- Qualification Criteria - Compliance**

Note to Bidders: Fill up this Form your past performance highlighting their qualification to supply relevant Equipment & Services as specified in qualification Criteria of Tender Document Section-VI. Statements and Documents to the Experience Statement may be mentioned/ attached here. Add additional details not covered elsewhere in your bid in this regard.

Order issued by (Complete address along with contact no.)	Purchase Order No. & Date	Project detail	Start Date of Project	Completion Date of Project	Project Value

Enclosure: Relevant Document Attached.

Yours faithfully,

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form5: Terms & Conditions- Compliance

(on Company Official Letter Head)

Bidder’s Name_________________

[Address and Contact Details]

Bidder’s Reference No.__________________

To

CEO, National Internet Exchange of India (NIXI), 9th
Floor, B-Wing, Statesman House,
148, Barakhamba Road, New Delhi 110001

Ref: Tender Document No. Tender No;

Subject: **Terms & Conditions - Compliance**

1) With reference to our Bid submitted against the above referred Tender no… , we hereby confirm that we comply with all terms, conditions and specifications of the Tender Documents read in conjunction with Amendment(s) / Clarification(s) (if any) issued by NIXI prior to last date of submission of bids and the same has been taken into consideration while submitting our bid and we declare that we have not taken any deviation in this regard.

2) We further confirm that any deviation, variation or additional conditions etc. or any mention, contrary to Bidding Documents and its Amendment(s)/ Clarification(s) (if any) as mentioned at 1.0 above found anywhere in our bid, implicit or explicit, shall stand unconditionally withdrawn, without any cost implication whatsoever to NIXI.

……………………..

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of

………………………………………

[name & address of Bidder and seal of company]

Form 6: Check-List for Bidders

(To be submitted as part of Technical bid) (on Company Letter-head)

Bidder's Name_________________

[Address and Contact Details]

Bidder's Reference No.__________________

Tender Document No. Tender No./ xxxx

Note to Bidders: This check-list is merely to help the bidders to prepare their bids, it does not over- ride or modify the requirement of the tender. Bidders must do their own due diligence also.

S.No.	Documents submitted, duly filled, signed	Yes/ No/ NA
1.	Form 1. Bid Form (to serve as covering letter and declarations applicable for both the Technical bid and Financial bid)	
2.	Form 1.1: Bidder Information along with Board Resolution/Power of attorney of authorizing signatories on stamp paper and Registration Certificates etc.	
2.a	Self-attested copy of Registration certificates etc. of the company	
2.b	Self-attested copy of PAN	
2.c	Self-attested copy of GSTIN registration(s)	
2.d	Self-attested copy of Power of Attorney etc. authorizing signatories on stamp paper to sign the bid	
3.	Form 1.2: Eligibility Declarations, along with supporting documents	
3.a	Self-attested copy of Registration certificate for bidders/ subcontractors from restricted neighboring countries, if any	
3.b	Self-attested copy of MSME registration	
3.c	Self-attested copy of Start-up registration/ status	
4.	Form 1.3: OEM's Authorization Form duly filled up	
4.a	Self-attested copy of Registration certificates etc. of the OEM	
5.	Form 2: Bill of Material – Compliance	
6.	Form 3: Technical Specifications - Compliance	
7.a	Relevant documents like technical data, literature, datasheets, drawings, and other relevant proposal/bid documents.	
7.	Form 4: Qualification Criteria – Compliance	

8.a	Documents Attached supporting the compliance to qualification criteria of Bidder and its OEM	
8.	Form 4.1: Experience Statement	
9.a	Documents/ contracts supporting the experience statement	
9.	Form 5: Terms and Condition compliance	
10.	Form 6: This Checklist	
11	Form 7: Documents relating to Bid Security	
12	Form 8: Duly signed Integrity Pact	
13	Form 9: Make In India Certificate	
14	Form 10: Non-Disclosure Agreement (To be submitted by successful Bidder only)	
15	**Unpriced** Schedule (Financial Bid(BOM)) as per Tender Document in Technical Bid	
17	Ink/digitally signed tender document along with its corrigendum/addendum	
18	Any other requirements, if stipulated in Tender Document or if considered relevant by the Bidder	
20	Documents if any at the option of Bidder	

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form 7: Documents Relating to Bid Security.

Note: To be submitted as part of Technical bid, along with supporting documents, if any. Bidders exempted from submission of bid security are also required to submit this.

Bid Securing Declaration

(on Company Letter-head) Bidder's

Name________________________

[Address and Contact Details]

Bidder's Reference No.__________________

To

CEO, National Internet Exchange of India (NIXI),
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road, New Delhi 110001

Ref: Tender Document No. Tender No./ xxxx;

Sir/ Madam

We, the undersigned, solemnly declare that:

We understand that according to the conditions of this Tender Document, the bid must be supported by a Bid Securing Declaration In lieu of Bid Security.

We unconditionally accept the conditions of this Bid Securing Declaration. We understand that we shall stand automatically suspended from being eligible for bidding in any tender in Procuring Organization for 2 years from the date of opening of this bid if we breach our obligation(s) under the tender conditions if we:

1) withdraw/ amend/ impair/ derogate, in any respect, from our bid, within the bid validity; or

2) being notified within the bid validity of the acceptance of our bid by the NIXI:

   refused to or failed to produce the original documents for scrutiny or the required Performance Security within the stipulated time under the conditions of the Tender Document.

We know that this bid-Securing Declaration shall expire if the contract is not awarded to us, upon:

1) receipt by us of your notification

   (a) of cancellation of the entire tender process or rejection of all bids or
   (b) of the name of the successful bidder or

2) forty-five days after the expiration of the bid validity or any extension to it.

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form 8: Integrity Pact

National Internet Exchange of India hereinafter referred to as "NIXI " And

---------------------------[bidder (s) participating in this tender] hereinafter referred to as
“The Bidder/Contractor”

Preamble

NIXI invites online bids (Tender for) for: Equipment(s) & Services

NIXI values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, NIXI will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for Compliance with the principles mentioned above.

Section 1- Commitments of NIXI

1. NIXI commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of NIXI, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
b. NIXI will during the tender process treat all Bidder(s) with equity and reason. NIXI will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder (s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.
c. NIXI will exclude from the process all known prejudiced persons.

2. If NIXI obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or it there be a substantive suspicion in this regard, NIXI will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) / Contractor(s)

1. The Bidder(s) / Contractor(s) commit himself to take all measures necessary to prevent corruption. The bidder commits himself to observe the following principles during his participation in the tender process and during the contract execution:

a. The Bidder(s) / contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of NIXI's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage or during the execution of the contract.

b. The Bidder(s) / Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non- submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
c. The Bidder(s) / Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) / Contractors will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by NIXI as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s) / Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers' as annexed and marked as Annexure.
e. The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from tender process and exclusion from future contracts

- If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, NIXI is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the Government/NIXI’s procedure on banning of the business dealings/bidders/contractors, etc.

Section 4: Compensation for Damages

a. If NIXI has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, NIXI is entitled to enforce Bid security Declaration.
b. If NIXI has terminated the contract according to section 3, or if NIXI is entitledto terminated the contract according to section 3, NIXI shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value and/or the amount equivalent to Performance Security or from any due payment to the bidder.

Section 5: Previous Transgression

a. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any other public sector enterprise in India that could justify his exclusion from the tender process.

b. If the bidder makes incorrect statement on this subject, he can be disqualified from the tender process for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders/Contractors/Subcontractors

a. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to NIXI before contract signing.
b. NIXI will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.
c. NIXI will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation Bidder(s)/ Contractor(s)/Sub contractor(s)

If NIXI obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if NIXI has substantive suspicion in this regard, NIXI will inform the same to the Chief Vigilance Officer, MeitY.

Section 8: Independent External Monitor/Monitors

1. NIXI appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Director General, NIXI.
3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of NIXI including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality.
4. NIXI will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between NIXI and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of NIXI and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The Monitor will submit a written report to the CEO NIXI within 8 to 10 weeks from the date of reference or intimation to him by NIXI and, should the arise, submit

proposals for correcting problematic situations.

7. Monitor shall be entitled to compensation on the same terms as being extended to / provided to by CEO NIXI.
8. If the Monitor has reported to CEO, NIXI, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CEO, NIXI has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
9. The word 'Monitor' would include both singular and plural

Section 9 - Pact Duration

1. This pact begins when both parties have legally signed it. It expires for the Contractor 10 months after the last payment under the contract or after 10 months from the expiry of Rate Contract (RC) which ever be later and for all other Bidders 12 months from the contract has been awarded.
2. If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CEO, NIXI.

Section 10 - Other provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered NIXI, i.e. New Delhi.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. Issues like Warranty/ Guarantee etc., shall be outside the purview of IEMs

(For & on behalf of NIXI)	(For & on behalf of Bidder)
(Office Seal)	(Office Seal)

Place_________

Date_________

Witness 1: (Name & Address)______________
Witness 2: (Name & Address)______________

Form 9 : Make in India Certificate

Make in India Certificate

(on Company Letter-head)

Bidder's Name_________________[Address and Contact Details]

Bidder's Reference No.__________________

Date……….

To

CEO, National Internet Exchange of India (NIXI)
9th Floor, B-Wing, Statesman House, 148,
Barakhamba Road,
New Delhi 110001

Ref: Tender Document No. Tender No./ xxxx;

(To be certified by statutory auditor or cost auditor of the company (in the case of companies) for a tender value above Rs. 10 crores giving the percentage of local content.)

In line with Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020 and its amendments, we hereby certify that we M/s______________________are local supplier meeting the requirement of minimum local content i.e.,___________% against NIXI Tender No…………………………………. dated…………………. . We qualify as a ____

(Class-I or Class II) local supplier. Details of location at which local value addition will be made as follows:_____________________________.

We also understand, false declarations will be in breach of the code of integrity under rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

[name & address of Bidder and seal of company]

Dated………………………..

Place……………………………………

Form 10: Non-Disclosure Agreement (To be submitted on Non-Judicial Stamp Paper of Rs 100/-)

This Agreement is made as on the___________, between National Internet Exchange of India called as "**NIXI**" through its ………………which expression shall unless repugnant to the subject or the context mean and include its successors, nominees or assigns.

and

<<< Contractor Name>>> called as "**-------------**" through its ------------------------- which expression shall unless repugnant to the subject or the context mean and include its successors, nominees or assigns.

NIXI and <<Contractor Name>> are sometimes referred to herein individually as "Party" and collectively as "Parties".

Tender No. ……………………. "Design, Supply, Installation, Testing, Commissioning, Operation & Maintenance of the Hardware & Software for Setting up of CCA SSL Root setup along with SSL CA setup at NIXI DC and DR Sites along with consultancy & all compliances for ensuring WebTrust certifications for the setup including incorporation of CCA Root for SSL in major web browsers. for O/o NIXI at **primary & secondary sites**" and Contract no……………………… **(**hereinafter referred as **"Project").** O/o NIXI and <<Contractor Name>> have entered into a contract to deliver this project, Now, both the parties enter into this agreement and agree that information provided and available with each party in respect of this project is to be used only for the specific project purpose and parties are required to protect such confidential information from unauthorized use and disclosure.

In consideration of the other party's disclosure of such information, each party agrees as follows:

1. This Agreement will apply to all confidential and proprietary information disclosed, owned or collected by one party to the other party, including information generated under this project, which the disclosing party identifies in writing or otherwise as confidential to the receiving party ("**Confidential information**"). Information consists of certain specifications, designs, plans, drawings and /or technical information, software, data etc, and all copies and derivatives containing such information, that may be disclosed to one another for and during the purpose, which a party considers proprietary or confidential ("**Information**"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to one party (hereinafter referred to as the receiving party) by the other party (hereinafter referred to as one disclosing party). Information shall be subject to this Agreement, if

it is in tangible form, only if clearly marked as proprietary or confidential as the case may be, when disclosed to the receiving party or, if not in tangible form, its proprietary nature must first be announced, and it must be reduced to writing and furnished to the receiving party.

2. NIXI and <<Contractor Name>>hereby agree that during and after the Agreement Period:

   a) The receiving party shall use Information only for the Purpose, shall hold Information in confidence using the same degree of care as it normally exercises to protect its own proprietary information, but not less than reasonable care, taking into account the nature of the Information, and shall grant access to Information only to its employees who have a need to know, but only to the extent necessary to carry out the business purpose of this project as defined, shall cause its employees, outsourced agencies, vendors, implementation partners and contract employees to comply with the provisions of this Agreement applicable to the receiving party, shall reproduce Information only to the extent essential for fulfilling the purpose, and shall prevent disclosure of information to third parties.

   b) Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been destroyed.

3. The foregoing restrictions on each party's use or disclosure of Information shall not apply to Information that the receiving party can demonstrate which: -

   a) was independently developed by or for the receiving party without reference to the Information, or was received without restrictions; or

   b) has become generally available to the public without breach of confidentiality obligations of the receiving party; or

   c) was in the receiving party's possession without restriction or was known by the receiving party without restriction in vogue at the time of disclosure; or

   d) is the subject of a subpoena or other legal or administrative stipulated requirement demand for disclosure; provided, however that the receiving party has given the disclosing party prompt notice of such requirement for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure and appropriate protective order; or

   e) is disclosed with the prior written consent of the disclosing party; or

   f) was in its possession or known to it by being in its use or being recorded in its files or computers or other recording media prior to receipt from the disclosing party and was not previously acquired by the receiving party from the disclosing party under an obligation of confidence; or

   g) the receiving party obtains or has available from a source other than the disclosing party without breach by the receiving party or such source of any obligation of confidentiality or non-use towards the disclosing party.

4. Each party agrees not to remove any of the other party's Confidential Information

from the premises and sites of the disclosing party without the disclosing party's prior written approval. Each party agrees to exercise extreme care in protecting the confidentiality of any confidential information which is removed, only with the disclosing party's prior written approval, from the disclosing party's premises and sites. Each party agrees to comply with any and all terms and conditions the disclosing party's may impose upon any such approved removal, such as conditions that the removed confidential information and all copies must be returned by a certain date, and that no copies are to be make off of the premises.

5. Upon the disclosing party's request, the receiving party will promptly return to the disclosing party all tangible items containing or consisting of the disclosing party's confidential information all copies thereof.
6. Each party recognizes and agrees that all of the disclosing party's confidential information is owned solely by the disclosing party (or its licensors) and that the unauthorized disclosure or use of such confidential information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain. Accordingly, each party agrees that the disclosing party will have the right to obtain an immediate injunction enjoining any breach of this agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity or may seek the intervention of Director General, NIXI for such a breach.
7. Access to information hereunder shall not preclude an individual who has seen such information for the purpose of this agreement from working on future projects for the receiving party which relate to similar subject matters provided that such individual does not make reference to the information and does not copy the substance of the information during the confidentiality period thereafter as required by applicable law. Furthermore, nothing contained herein shall be construed as imposing any restriction on the receiving party's disclosure or use of any general learning, skills or know how developed by the receiving party's personnel under this agreement, if such disclosure and use would be regarded by a person of ordinary skill in the relevant area as not constituting a disclosure or use of the information.
8. As between the parties, all information shall remain the property of the disclosing party. By disclosing information or executing this agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection rights, trade secret or any other intellectual property right. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINNIXIENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this agreement and the disclosure of information pursuant to this agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase, or sale or to enter into any additional agreement of any kind.

9. Either party’s failure to enforce any provision, right or remedy under this agreement shall not constitute a waiver of such provision, right or remedy.
10. This Agreement will be construed in, interpreted and applied in accordance with the laws of India.
11. That in case of any dispute or differences, breach & violation relating to the terms of this agreement, the said matter or dispute, difference shall be referred to Controller, NIXI for his decision in this regard. The decision of the Controller, NIXI will be final and binding on both the parties.
12. This Agreement constitutes the entire agreement of the parties with respect to the parties respective obligations in connection with Information disclosed hereunder and supersedes all prior oral and written agreements and discussions with respect thereto.
13. The parties can amend or modify this agreement only by a writing duly executed by their respective authorized representatives. Neither party shall assign this Agreement without first securing the other Party’s written consent.
14. This Agreement will remain in effect during the currency of agreement & shall survive even after expiry of the agreement or project.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by Their duly authorized officers or representatives.

For and on behalf of	For and on behalf of
National Internet Exchange of India	<< Contractor Name>>
<< Authorized Signatory >>	<< Authorized Signatory >>
Name:	Name:
Designation:	Designation:
NIXI, Delhi	<<Contractor Name>>
:	

FORMATS

Format 1.1: Bank Guarantee Format for Performance Security

(To be stamped in accordance with stamp Act)
(The non-judicial stamp paper should be in the name of issuing Bank)

To,

CEO, National Internet Exchange of India (NIXI)
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road,
New Delhi 110001

Dear Sirs,

In consideration of the NIXI, Department of Electronics & Information Technology Ministry of Communications & Information Technology (hereinafter referred as the **'Owner'**, which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns) having awarded to M/s.________(name and address) (herein referred to as the '**Contractor**', which expression shall unless repugnant to the context of meaning thereof, include its successors, administrator, executors and assigns) a Purchase Order No.____ and the Contractor having agreed to provide a Bank Guarantee towards Performance of the entire Contract equivalent to Rs.__(amount of BG) (i.e.__per cent of the said value of the Contract) to the Owner.

We______(name of the Bank) having its Registered Office at_____and Corporate/Head Office at_____________________________(hereinafter referred to as the 'Bank', which expression shall, unless repugnant to the context or meaning thereof, include the successors, administrators, executors and assigns) do hereby guarantee and undertake to pay at any time up to_______(day/month/year including claim period) an amount not exceeding Rs.________, within ten (10) calendar days from the date of receipt by us on first written demand by Owner; through hand delivery or registered A.D. Post or by speed post or by courier, stating that "Contractor" has failed to perform its obligations under the Contract. Aforesaid payment will be made without any demur, reservation, contest, recourse or protest and/or without any reference to the Contractor. Any such demand made by the owner the Bank shall be conclusive and binding notwithstanding any difference between the Owner and Contractor or any dispute pending before any court, tribunal or any authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the Owner and further agrees that the guarantee herein contained shall continue to be enforceable till the Owner discharges this guarantee. The owner shall have the fullest liberty,

without affecting in any way the liability of the Bank under this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Contractor, and to exercise the same at any time in any manner, and either to enforce or to forebear to enforce any covenants, contained or implied, in the Contract between the Owner and the Contractor or any other course of or remedy or security available to the Owner. The Bank shall not be relieved of its obligations under these presents by any exercise by the owner or by any other matters or thing whatsoever which under law would, but for this provision, have the effect of relieving the Bank. The Bank also agrees that the Owner at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Contractor and notwithstanding any security or other guarantee that the Owner may have in relation to the Contractors liabilities.

This Guarantee can be invoked in one or more trenches and in such a case Owner will not be required to submit the original Guarantee along with submission of claim.

Notwithstanding anything mentioned herein above our liability under this guarantee is restricted to Rs.___________and it shall remain in force up to and including_________shall be extended from time to time for such period as may be desired by the Contractor on whose behalf this guarantee has been issued.

WITNESS
Signature_________________

BANK
Signature______________

Name______________________

Name________________

Designation with Bank Stamp
Address of the Bank Branch

Format 1.2: No Claim Certificate

(On company Letter-head) Contractor’s

Name___________________________

[Address and Contact Details]_____________________

Contractor’s Reference No.__________________

To,

CEO, National Internet Exchange of India (NIXI)
9th Floor, B-Wing, Statesman House,
148, Barakhamba Road,
New Delhi 110001

No Claim Certificate

Sub: Contract Agreement no.________________dated ________________

Sir/Madam,

We have received the sum of Rs. (Rupees________________________ ____only) as final settlement due to us for the supply of_____________________under the abovementioned contract agreement.

We have received all the amounts payable to us with this payment and have no outstanding dispute of any description whatsoever regarding the amounts worked out as payable to us and received by us.

We hereby unconditionally and without any reservation whatsoever, certify that we shall have no further claim whatsoever, of any description, on any account, against the NIXI, under contract above. We shall continue to be bound by the terms and conditions of the contract agreement regarding its performance.

Yours faithfully,

Signatures of contractor or officer authorized

to sign the contract documents on behalf of the

contractor (company Seal)

Date:_______________Place:____________

Format 2: Authorization for Attending Pre-bid Conference.

(on Company Official Letter Head)

Bidder’s Name__________[Address and Contact Details]

Bidder’s Reference No._________________________

Ref: Tender Document No. Tender No./ xxxx;

Subject: Authorization for attending Pre-bid Conference on____________________(date).

Following persons are hereby authorized to attend the Pre-bid Conference for the tender mentioned above on behalf of____(Bidder) in order of preference given below.

Sr.No	**Name**	**Government Photo ID Type/ Number**
I.		
II.		
Alternate Representative		

Note:

1. Maximum of two representatives (carrying valid Government photo IDs) shall be permitted to attend the Pre-bid. An alternate representative shall be permitted when regular representatives are not able to attend.

2. Permission to enter the hall / e-Meeting where the pre-bid conference is conducted may be refused if authorization as prescribed above is not submitted.

Signatures of bidder or Officer authorized to sign the bid. Documents on behalf of the bidder
Dated………………………………
Place……………………………….

[name & address of Bidder and seal of company]

(Signature with date)

………………………..

(Name and designation)

Duly authorized to sign bid for and on behalf of……………………….

Annexure I

CHECK-LIST

The confirmation to the following should be provided to ensure the following requirements/ controls have been included in the comprehensive solution including CA architecture & Design, sites construction, CA setup, operation & maintenance, all categories of audit, man power resource allocation, data synchronization, business continuity, third part contract etc. offered by the bidder.

SL	REQUIREMENTS/CONTROLS	CONFIRM (Y/N)
0.1	Internal RA is offered	
0.2	CA model is Standard hierarchical	
0.3	The Certification Authority: • Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement; and • Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy (if applicable).	
0.4	The CA maintains effective controls to provide reasonable assurance that: • The CA's Certification Practice Statement is consistent with its Certificate Policy (if applicable); and • The CA provides its services in accordance with its Certificate Policy (if applicable) and Certification Practice Statement.	
0.5	These WebTrust Principles and Criteria for Certification Authorities v2.2.1 recommend CAs to structure their CP and CPS documents in accordance with *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003*. The use of *IETF RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999* is still permitted to be used, although CAs still using RFC 2527 should transition to RFC 3647 as the use of RFC 2527 may be deprecated in future releases of these Criteria. The use of any other framework for business practice disclosures is no longer permitted in these Criteria.	
0.6	The CA maintains effective controls to provide reasonable assurance that: • The integrity of keys and certificates it manages is established and protected throughout their life cycles; • The Subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and • Subordinate CA certificate requests are accurate, authenticated and approved.	
0.7	The user certificate life cycle is at the core of the services provided by the CA. The CA establishes its standards and practices by which it will deliver services in its published CPS and Certificate Policy(s). The user certificate life cycle includes the following:	

	• Registration (meaning, the identification and authentication process related to binding the individual subscriber to the certificate); • The renewal of certificates (if applicable); • The rekey of certificates; • The revocation of certificates; • The suspension of certificates (if applicable); • The timely publication of certificate status information (through Certificate Revocation Lists or some form of online certificate status protocol) • The management of integrated circuit cards (ICCs) holding private keys through their life cycle (if applicable); • The registration, issuance and management of subordinate CA certificates	
0.8	The Certification Authority maintains effective controls to provide reasonable assurance that: • Logical and physical access to CA systems and data is restricted to authorised individuals; • The continuity of key and certificate management operations is maintained; and • CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity.	
0.9	The Certification Authority: • Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement; • Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy (if applicable); and • Provides services in accordance with its disclosed practices.	
1.1	Certification Practice Statement (CPS) The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certification Practice Statement.	
1.2	Certificate Policy (CP) (if applicable) The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certificate Policy. *Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, or it implements the CP defined by another CA, then Criterion 1.2 is not applicable.*	1

2.0	CA Business Practices Management The Certification Authority maintains effective controls to provide reasonable assurance that: • The CA provides its services in accordance with its Certification Practice Statement and Certificate Policy (if applicable); • The CA's Certification Practice Statement is consistent with its Certificate Policy (if applicable).	
2.1	Certification Practice Statement (CPS) Management The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.	
2.1.1	The PA has final authority and responsibility for approving the CA's Certification Practice Statement (CPS).	
2.1.2	Responsibilities for maintaining the CPS have been formally assigned.	
2.1.3	The CA's CPS is modified and approved in accordance with a defined review process.	
2.1.4	The CA makes available its Certification Practice Statement (CPS) to all appropriate parties.	
2.1.5	Revisions to the CA's CPS are made available to appropriate parties.	
2.1.6	The CA updates its CPS to reflect changes in the environment as they occur.	
2.2	Certificate Policy (CP) Management (if applicable) The CA maintains controls to provide reasonable assurance that its Certificate Policy (CP) management process is effective. *Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, or it implements the CP defined by another CA, then Criterion 2.2 is not applicable.*	
2.2.1	The Policy Authority (PA) has the responsibility of defining the business requirements and policies for using digital certificates and specifying them in a Certificate Policy (CP) and supporting agreements.	
2.2.2	The PA has final authority and responsibility for specifying and approving Certificate Policy(s).	
2.2.3	Certificate Policy(s) are approved by the Policy Authority in accordance with a defined annual review process, including responsibilities for maintaining and tracking changes to the Certificate Policy(s).	
2.2.4	A defined review process exists to assess that the Certificate Policy(s) are capable of support by the controls specified in the CPS.	
2.2.5	The PA makes available the Certificate Policies supported by the CA to Subscribers and Relying Parties.	
2.3	CP and CPS Consistency (if applicable) The CA maintains controls to provide reasonable assurance that its Certification Practice Statement addresses the topics included in its Certificate Policy. *Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, then Criterion 2.3 is not applicable. However, if the CA implements the CP defined by another CA, then this criterion is relevant for ensuring the CA's developed CPS is consistent with the provided CP.*	
2.3.1	The PA is responsible for ensuring that the CA's control processes, as stated in a	

	Certification Practice Statement (CPS) or equivalent, fully comply with the requirements of the CP.	
2.3.2	The CA addresses the requirements of the CP when developing its CPS.	
2.3.3	The CA assesses the impact of proposed CPS changes to ensure that they are consistent with the CP.	
2.3.4	A defined review process exists to ensure that Certificate Policy(s) are supported by the CA's CPS.	
3.0	CA Environmental Controls The Certification Authority maintains effective controls to provide reasonable assurance that: • Logical and physical access to CA systems and data is restricted to authorised individuals; • The continuity of key and certificate management operations is maintained; and • CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity.	
3.1	Security Management The CA maintains controls to provide reasonable assurance that: • security is planned, managed and supported within the organization; • security risks are identified and managed; • the security of CA facilities, systems and information assets accessed by third parties is maintained; and the security of subscriber and relying party information is maintained when the responsibility for CA sub-functions has been outsourced to another organisation or entity.	
3.1.1	An information security policy document, that includes physical, personnel, procedural and technical controls, is approved by management, published and communicated to all employees.	
3.1.2	Responsible management of the CA demonstrates that the information security policy is implemented and adhered to.	
3.1.3	The information security policy includes the following: a) a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing; b) a statement of management intent, supporting the goals and principles of information security; c) an explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation; d) a definition of general and specific responsibilities for information security management, including reporting security incidents; and references to documentation, which supports the policy.	
3.1.4	There is a defined review process for maintaining the information security policy, including responsibilities and review dates.	
3.1.5	Senior management and/or a high-level management information security	

	committee have the responsibility to ensure there is clear direction and management support to manage risks effectively.	
3.1.6	A management group or security committee exists to co-ordinate the implementation of information security controls and the management of risk.	
3.1.7	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.	
3.1.8	A management authorisation process for new information processing facilities exists and is followed.	
3.1.9	Procedures exist and are enforced to control physical and logical access to CA facilities and systems by third parties (e.g., on-site contractors, trading partners and joint ventures).	
3.1.10	If there is a business need for the CA to allow third party access to CA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements.	
3.1.11	Arrangements involving third party access to CA facilities and systems are based on a formal contract containing necessary security requirements.	
3.1.12	If the CA outsources the management and control of all or some of its information systems, networks, and/or desktop environments, the security requirements of the CA are addressed in a contract agreed upon between the parties.	
3.1.13	If the CA chooses to delegate a portion of the CA roles and respective functions to another party, the CA maintains responsibility for the completion of the outsourced functions and the definition and maintenance of a statement of its CPS.	
3.2	Asset Classification and Management The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.	
3.2.1	Owners are identified for all CA assets and assigned responsibility for the protection of the assets.	
3.2.2	Inventories of CA assets are maintained.	
3.2.3	The CA has implemented information classification and associated protective controls for information based on business needs and the business impacts associated with such needs.	
3.2.4	Information labelling and handling are performed in accordance with the CA's information classification scheme and documented procedures.	
3.3	Personnel Security The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	
3.3.1	The CA employs personnel (i.e., employees and contractors) who possess the relevant skills, knowledge and experience required for the job function.	
3.3.2	Security roles and responsibilities, as specified in the organisation's security policy, are documented in job descriptions.	
3.3.3	Trusted Roles, on which the security of the CA's operation is dependent, are clearly identified. Trusted roles include, at a minimum, the following responsibilities: a) overall responsibility for administering the implementation of the CA's security practices; b) approval of the generation, revocation and suspension of certificates; c) installation, configuration and maintenance of the CA systems; d) day-to-day operation of CA systems and system backup and recovery; e) viewing and maintenance of CA system archives and audit logs; f) cryptographic key life cycle management functions (e.g., key component	

	custodians); and CA systems development.	
3.3.4	The CA’s policies and procedures specify the background checks and clearance procedures required for Trusted Roles and non-trusted roles. As a minimum, verification checks on permanent staff are performed at the time of job application and periodically for those individuals undertaking Trusted Roles.	
3.3.5	An individual’s trusted status is approved prior to gaining access to systems/facilities or performing actions requiring trusted status.	
3.3.6	CA Employees and Trusted Roles sign a confidentiality (non-disclosure) agreement as a condition of employment.	
3.3.7	Contractors who perform Trusted Roles are subject to at least the same background check and personnel management procedures as employees.	
3.3.8	Any contract arrangement between Contractors and CAs allows for the provision of temporary contract personnel that explicitly allows the organisation to take measures against contract staff who violate the organisation’s security policies. Protective measures may include: a) bonding requirements on contract personnel; b) indemnification for damages due to contract personnel willful harmful actions; and financial penalties.	
3.3.9	Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management.	
3.3.10	A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The CA’s policies and procedures specify the sanctions against personnel for unauthorised actions, unauthorized use of authority, and unauthorized use of systems.	
3.3.11	Physical and logical access to CA facilities and systems is disabled upon termination of employment.	
3.3.12	If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.	
3.3.13	All employees of the organisation and, where relevant, third party contractors, receive appropriate training in organisational policies and procedures. The CA’s policies and procedures specify the following: a) The training requirements and training procedures for each role; and Any retraining period and retraining procedures for each role.	
3.3.10	A formal disciplinary process exists and is followed for employees who have violated organisational security policies and procedures. The CA’s policies and procedures specify the sanctions against personnel for unauthorised actions, unauthorised use of authority, and unauthorised use of systems.	
3.4	Physical and Environmental Security The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented. *Explanatory Guidance: ‘Dual Custody Control’ requires the CA to have controls in place to require at least two trusted people be present during the duration of the authorised activity in order to physically access CA systems. An example of this is*	

	an access control system requiring two people to each present their badges and second factor (i.e. biometrics, PIN) prior to access being granted to the facility.	
3.4.1	Entry to the building or site containing the CAs certificate manufacturing facility is achieved only through a limited number of controlled access points.	
3.4.2	All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organisation’s other systems so that only authorised employees of the CA can access them.	
3.4.3	A manned reception area or other means to control physical access is in place to restrict access to the building or site housing CA operations to authorised personnel only.	
3.4.4	Physical barriers are in place (e.g., solid walls that extend from real floor to real ceiling) to prevent unauthorised entry and environmental contamination to the CAs certificate manufacturing facility.	
3.4.5	Physical barriers are in place (e.g., Faraday cage) to prevent electromagnetic radiation emissions for all Root CA operations (e.g., key generation and certification of CA Certificates) as disclosed in CP and/or CPS.	
3.4.6	Fire doors exist on security perimeters around CA operational facilities and are alarmed and conform to local fire regulations.	
3.4.7	Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the CA operational facilities.	
3.4.8	CA operational facilities are physically locked and alarmed when unoccupied.	
3.4.9	All personnel are required to wear visible identification. Employees are encouraged to challenge anyone not wearing visible identification.	
3.4.10	Access to CA operational facilities is controlled and restricted to authorised persons through the use of multi-factor authentication controls.	
3.4.11	All personnel entering and leaving CA operational facilities are logged (i.e., an audit trail of all access is securely maintained).	
3.4.12	Entry, exit, and activities within CA facilities are monitored by cameras.	
3.4.13	Visitors to CA facilities are supervised and their date and time of entry and departure recorded.	
3.4.14	Third party support services personnel is granted restricted access to secure CA operational facilities only when required and such access is authorised and accompanied.	
3.4.15	Access rights to CA facilities are regularly reviewed and updated.	
3.4.16	The CA maintains an equipment inventory.	
3.4.17	Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	
3.4.18	Equipment is protected from power failures and other electrical anomalies.	
3.4.19	Power and telecommunications, within the facility housing the CA operation, cabling carrying data or supporting CA services is protected from interception or damage.	
3.4.20	Equipment is maintained in accordance with the manufacturer’s instructions and/or other documented procedures.	
3.4.21	All items of equipment containing storage media (fixed and removable disks) are checked to ensure that they do not contain sensitive data prior to their disposal. Storage media containing sensitive data is physically destroyed or securely overwritten prior to disposal or reused.	
3.4.22	Sensitive or critical business information is locked away when not required and when the CA facility is vacated.	
3.4.23	Procedures require that personal computers and workstations are logged off or protected by key locks, passwords or other controls when not in use.	
3.4.24	The movement of materials to/from the CA facility requires prior authorisation.	
3.5	Operations Management The CA maintains controls to provide reasonable assurance that:	

	• the secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimised; • the integrity of CA systems and information is protected against viruses and malicious software; • damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and media are securely handled to protect them from damage, theft and unauthorised access.	
3.5.1	CA operating procedures are documented and maintained for each functional area.	
3.5.2	Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures.	
3.5.3	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.	
3.5.4	Development and testing facilities are separated from operational facilities.	
3.5.5	Prior to using external facilities management services, risks and related controls are identified, agreed upon with the contractor, and incorporated into the contract.	
3.5.6	Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.	
3.5.7	Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system carried out prior to acceptance.	
3.5.8	Detection and prevention controls to protect against viruses and malicious software, including on offline or air gapped systems are implemented. Employee awareness programs are in place.	
3.5.9	A formal security incident reporting procedure exists setting out the actions to be taken on receipt of an incident report. This includes a definition and documentation of assigned responsibilities and escalation procedures. Any incidents are reported to responsible management as a matter of urgency.	
3.5.10	Users of CA systems are required to note and report observed or suspected security weaknesses in, or threats to, systems or services as they are detected.	
3.5.11	Procedures exist and are followed for reporting hardware and software malfunctions.	
3.5.12	Procedures exist and are followed to assess that corrective action is taken for reported incidents.	
3.5.13	A formal problem management process exists that allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified and monitored.	
3.5.14	Procedures for the management of removable computer media require the following: a) if no longer required, the previous contents of any reusable media that are to be removed from the organisation are erased or media is destroyed; b) authorisation is required for all media removed from the organisation and a record of all such removals to maintain an audit trail is kept; and all media are stored in a safe, secure environment, in accordance with manufacturers' specifications.	
3.5.15	Equipment containing storage media (i.e., fixed hard disks) is checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information are physically destroyed or securely overwritten prior to disposal or reuse.	
3.5.16	Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorised disclosure or misuse.	
3.5.17	System documentation is protected from unauthorised access.	
3.6	System Access Management	

	The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that: • hypervisor, operating system, database, and network device access is limited to authorised individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorised individuals, applications and services; and CA application use is limited to authorised individuals.	
3.6.1	Business requirements for access control are defined and documented in an access control policy that includes at least the following: a) roles and corresponding access permissions; b) identification and authentication process for each user; c) segregation of duties; and number of persons required to perform specific CA operations (i.e., m of n rule where m represents the number of key shareholders required to perform an operation and n represents the total number of key shares).	
3.6.2	There is a formal user registration and de-registration procedure for access to CA information systems and services, including hypervisors, operating systems, database, and network devices.	
3.6.3	The allocation and use of privileges is restricted and controlled.	
3.6.4	The allocation of passwords and multi-factor authentication tokens is controlled through a formal management process.	
3.6.5	Access rights for users with trusted roles are reviewed at regular intervals and updated.	
3.6.6	Users are required to follow defined policies and procedures in the selection and use of passwords.	
3.6.7	Users are required to ensure that unattended equipment has appropriate protection.	
3.6.8	Where technically feasible, administrative and superuser accounts require the use of multi- factor authentication controls.	
3.6.9	CA employed personnel are provided direct access only to the services that they have been specifically authorised to use. The path from the user terminal to computer services is controlled.	
3.6.10	Remote access to CA systems, made by CA employees or external systems, if permitted, requires authentication.	
3.6.11	Connections made by CA employees or CA systems to remote computer systems are authenticated.	
3.6.12	Access to diagnostic ports is securely controlled.	
3.6.13	Controls (e.g., firewalls) are in place to protect the CA’s internal network domain from any unauthorised access from any other domain.	
3.6.14	Controls are in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorised users in accordance with the CA’s access control policies. The security attributes of all network services used by the CA organisation are documented by the CA.	
3.6.15	Routing controls are in place to ensure that computer connections and information flows do not breach the CA’s access control policy.	
3.6.16	The CA maintains local network components (e.g., firewalls and routers) in a physically secure environment and audits their configurations periodically for compliance with the CA’s configuration requirements.	
3.6.17	Sensitive data is encrypted when exchanged over public or untrusted networks.	
3.6.18	Hypervisors, operating systems, databases, and network devices are configured in accordance with the CA’s system configuration standards and periodically reviewed and updated.	

3.6.19	Hypervisors, operating system, database, and network device patches and updates are applied in a timely manner when deemed necessary based on a risk assessment and follow formal change management procedures (see § 3.7).	
3.6.20	Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.	
3.6.21	Access to CA systems requires a secure logon process.	
3.6.22	All CA personnel users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. Where shared or group accounts are required, other monitoring controls are implemented to maintain individual accountability.	
3.6.23	Uses of system utility programs are restricted to authorised personnel and tightly controlled.	
3.6.24	Inactive terminals serving CA systems require re-authentication prior to use.	
3.6.25	Restrictions on connection times are used to provide additional security for high-risk applications.	
3.6.26	Sensitive data is protected against disclosure to unauthorised users.	
3.6.27	Access to information and application system functions is restricted in accordance with the CA's access control policy.	
3.6.28	CA personnel are successfully identified and authenticated before using critical applications related to certificate management.	
3.6.29	Sensitive systems (e.g., Root CA) require a dedicated (isolated) computing environment.	
3.7	Systems Development, Maintenance, and Change Management The CA maintains controls to provide reasonable assurance that CA systems development, maintenance activities, patching, and changes to CA systems including hypervisors (where applicable), operating systems, databases, applications, network devices, and hardware are documented, tested, authorised, and properly implemented to maintain CA system integrity.	
3.7.1	Business requirements for new systems, or enhancements to existing systems specify the control requirements.	
3.7.2	Software testing and change control procedures exist and are followed for the implementation of software on operational systems including scheduled software releases, modifications, patches, and emergency software fixes.	
3.7.3	Change control procedures exist and are followed for the hardware, network component, and system configuration changes.	
3.7.4	Test data is protected and controlled.	
3.7.5	Control is maintained over access to program source libraries.	
3.7.6	Application systems are reviewed and tested when operating system changes occur.	
3.7.7	The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems.	
3.7.8	Modifications to software packages are discouraged and all changes are strictly controlled.	
3.7.9	The purchase, use and modification of software are controlled and checked to protect against possible covert channels and Trojan code. This includes the authentication of the source of the software. These controls apply equally to outsourced software development.	
3.8	Disaster Recovery, Backups, and Business Continuity Management The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;	

	• creating backups of systems, data, and configuration information at regular intervals in accordance with the CA’s disclosed business practices, and storage of these backups at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA’s services.	
3.8.1	The CA has a managed process for developing and maintaining its business continuity plans. The CA has a business continuity planning strategy based on an appropriate risk assessment.	
3.8.2	The CA has a business continuity plan to maintain or restore the CA’s operations in a timely manner following interruption to, or failure of, critical CA processes. The CA’s business continuity plan addresses the following: a) the conditions for activating the plans; b) emergency procedures; c) fall-back procedures; d) resumption procedures; e) a maintenance schedule for the plan; f) awareness and education requirements; g) the responsibilities of the individuals; h) recovery time objective (RTO) and recovery point objective (RPO); and regular testing of contingency plans.	
3.8.3	The CA’s business continuity plans include disaster recovery processes for all critical components of a CA system, including the hardware, software and keys, in the event of a failure of one or more of these components. Specifically: a) cryptographic devices used for storage of backup CA private keys are securely stored at an off-site location in order for the CA to recover in the event of a disaster at the primary CA facility; and the requisite secret key shares or key components, needed to use and manage the disaster recovery cryptographic devices, are securely stored at an off-site location.	
3.8.4	Backup copies of essential business information are regularly taken. The security requirements of these copies are consistent with the controls for the information backed up.	
3.8.5	The CA identifies and arranges for an alternate site where core PKI operations can be restored in the event of a disaster at the CA’s primary site. Fall-back equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site.	
3.8.6	The CA’s business continuity plans include procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.	
3.8.7	The CA’s business continuity plans address the recovery procedures used when computing resources, software, and/or data are corrupted or suspected to be corrupted.	
3.8.8	Business continuity plans are tested regularly to ensure that they are up to date and effective.	
3.8.9	Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CP and/or CPS.	
3.8.10	Business continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness.	
3.8.11	The CA maintains procedures for the termination, notification of affected entities, and for transferring relevant archived CA records to a custodian as disclosed in the	

	CP and/or CPS.	
3.9	Monitoring and Compliance The CA maintains controls to provide reasonable assurance that: • it conforms with the relevant legal, regulatory and contractual requirements; • compliance with the CA’s security policies and procedures is ensured; • the effectiveness of the system audit process is maximised and interference to and from the system audit process is minimised; and • unauthorised CA system usage is detected. *Explanatory Guidance: This Criterion addresses the existence of controls and business processes the CA has in place to help ensure it complies with all relevant legal requirements. An example would be testing if a framework is in place to help track requirements and monitor compliance. However, a practitioner would not test if the CA is actually in compliance with its legal requirements, and no assurance over the CA’s compliance status can be provided.*	
3.9.1	Relevant statutory, regulatory and contractual requirements are explicitly defined and documented.	
3.9.2	The CA has implemented procedures to comply with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.	
3.9.3	Controls are in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic hardware and software.	
3.9.4	Procedures exist to ensure that personal information is protected in accordance with relevant legislation.	
3.9.5	The information security policy addresses the following: a) the information that must be kept confidential by CA or RA; b) the information that is not considered confidential; c) the policy on release of information to law enforcement officials; d) information that can be revealed as part of civil discovery; e) the conditions upon which information may be disclosed with the subscriber’s consent; and any other circumstances under which confidential information may be disclosed.	
3.9.6	CA records are protected from loss, unauthorised destruction and falsification.	
3.9.7	Management authorises the use of information processing facilities and controls are applied to prevent the misuse of such facilities.	
3.9.8	Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.	
3.9.9	The CA’s operations are subject to regular review to ensure timely compliance with its CPS.	
3.9.10	CA systems are periodically checked for compliance with security implementation standards.	
3.9.11	Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.	
3.9.12	Access to system audit tools is protected to prevent possible misuse or compromise.	
3.9.13	Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorised or suspicious activity. Alerting mechanisms are implemented to detect unauthorised access.	
	Criterion	
3.10	Audit Logging	

	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and audit logs are reviewed periodically by authorised personnel.	
3.10.1	The CA generates automatic (electronic) and manual audit logs in accordance with the requirements of the CP and/or CPS.	
3.10.2	All journal entries include the following elements: a) date and time of the entry; b) serial or sequence number of entry (for automatic journal entries); c) kind of entry; d) source of entry (e.g., terminal, port, location, customer, etc.); and identity of the entity making the journal entry.	

3.10.3	The CA logs the following CA key life cycle management related events:
	a) CA key generation;
	b) installation of manual cryptographic keys and its outcome (with the identity of the operator);
	c) CA key backup;
	d) CA key storage;
	e) CA key recovery;
	f) CA key escrow activities (if applicable);
	g) CA key usage;
	h) CA key archival;
	i) withdrawal of keying material from service;
	j) CA key destruction;
	k) CA key transportation;
	l) CA key migration
	m) identity of the entity authorising a key management operation;
	n) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media);
	o) custody of keys and of devices or media holding keys; and
	compromise of a private key.	

3.10.4	The CA logs the following cryptographic device life cycle management related events: a) device receipt and installation; b) placing into or removing a device from storage; c) device activation and usage; d) device de-installation; e) designation of a device for service and repair; and device retirement.	
3.10.6	The CA records (or requires that the RA record) the following certificate application information: a) the method of identification applied and information used to meet subscriber requirements;	

	b) record of unique identification data, numbers, or a combination thereof (e.g., applicants drivers license number) of identification documents, if applicable; c) storage location of copies of applications and identification documents; d) identity of entity accepting the application; e) method used to validate identification documents, if any; f) name of receiving CA or submitting RA, if applicable; g) the subscriber’s acceptance of the Subscriber Agreement; and where required under privacy legislation, the Subscriber’s consent to allow the CA to keep records containing personal data, pass this information to specified third parties, and publication of certificates.	
3.10.7	The CA logs the following certificate life cycle management related events: a) receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests; b) submissions of public keys for certification; c) change of affiliation of an entity; d) generation of certificates; e) distribution of the CA’s public key; f) certificate revocation requests; g) certificate revocation; h) certificate suspension requests (if applicable); i) certificate suspension and reactivation; and generation and issuance of Certificate Revocation Lists.	
3.10.8	The CA logs the following security-sensitive events: a) security-sensitive files or records read or written including the audit log itself; b) actions taken against security-sensitive data; c) security profile changes; d) use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); e) system crashes, hardware failures and other anomalies; f) actions taken by individuals in Trusted Roles, computer operators, system administrators, and system security officers; g) change of affiliation of an entity; h) decisions to bypass encryption/authentication processes or procedures; and access to the CA system or any component thereof.	
3.10.9	Audit logs do not record the private keys in any form (e.g., plaintext or enciphered).	
3.10.10	CA computer system clocks are synchronised for accurate recording as defined in the CP and/or CPS that specifies the accepted time source.	
3.10.11	Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorised destruction.	
3.10.12	Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.	
3.10.13	The private key used for signing audit logs is not used for any other purpose. This applies equally to a symmetric secret key used with a symmetric MAC mechanism.	
3.10.14	The CA archives audit log data on a periodic basis as disclosed in the CP and/or CPS.	
3.10.15	In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.	
3.10.16	The CA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.	
3.10.11	Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorised destruction.	

3.10.12	Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.	
3.10.13	The private key used for signing audit logs is not used for any other purpose. This applies equally to a symmetric secret key used with a symmetric MAC mechanism.	
3.10.14	The CA archives audit log data on a periodic basis as disclosed in the CP and/or CPS.	
3.10.15	In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.	
3.10.16	The CA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.	
3.10.17	Current and archived audit logs are only retrieved by authorised individuals for valid business or security reasons.	
3.10.18	Audit logs are reviewed periodically according to the practices established in the CPS. The review of current and archived audit logs include a validation of the audit logs' integrity, and the timely identification and follow up of unauthorised or suspicious activity.	
4.0	4.0: CA Key Lifecycle Management Controls The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.	
4.1	CA Key Generation The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts. The CA's disclosed business practices include but are not limited to: a) generation of CA keys are undertaken in a physically secured environment (see §3.4); b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge; c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS; d) generation of CA keys are witnessed by an independent party and/or videotaped; and e) CA key generation activities are logged. The CA key generation script includes the following: a) definition of roles and participant responsibilities; b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony; d) specific steps performed during the key generation ceremony; e) physical security requirements for the ceremony location; f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; g) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and notation of any deviations from the key generation ceremony script.	

4.1.1	Generation of CA keys occur within a cryptographic module meeting the applicable requirements of ISO 19790 and ISO 13491-1/FIPS 140-2 (or equivalent)/ANSI X9.66 and the business requirements in accordance with the CPS. Such cryptographic devices perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG).	
4.1.2	The CA generates its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device where it will be used.	
4.1.3	CA key generation generates keys that:	
	use a key generation algorithm as disclosed within the CA's CP and/or CPS; have a key length that is appropriate for the algorithm and for the validity period of the CA certificate as disclosed in the CA's CP and/or CPS. The public key length to be certified by a CA is less than or equal to that of the CA's private signing key; and take into account requirements on parent and subordinate CA key sizes and have a key size in accordance with the CA's CP and/or CPS.	
4.1.4	CA key generation ceremonies are independently witnessed by internal or external auditors.	
4.1.5	Generation of CA keys shall be undertaken in a physically secured environment (see §3.4) by personnel in trusted roles (see §3.3) under the principles of multiple control and split knowledge.	
4.1.6	The CA follows a CA key generation script for key generation ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key generation ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers; d) specific steps performed during the key generation ceremony, including; • Hardware preparation; • Verification of the integrity of the operating system and other software from its source (e.g. through the use of hash totals); • When a previously built master operating system image is being used, verification of the integrity of that image; • Operating system installation; • CA application installation and configuration; • CA key generation; • CA key backup; • CA certificate signing; • CA system shutdown; and • Preparation of materials for storage. e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony (e.g., detailing the allocation of materials between storage locations); g) sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and notation of any deviations from the key generation ceremony script (e.g., documentation of steps taken to address any technical issues).	
4.1.7	The integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage.	
4.2	CA Key Storage, Backup, and Recovery The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed	

	up, stored and recovered by authorised personnel in trusted roles, using multiple person control in a physically secured environment.	
4.2.1	The CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or FIPS 140-2 level requirement based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable Certificate Policy(s).	
4.2.2	If the CA's private keys are not exported from a secure cryptographic module, then the CA private key is generated, stored and used within the same cryptographic module.	
4.2.3	If the CA's private keys are exported from a secure cryptographic module to secure storage for purposes of offline processing or backup and recovery, then they are exported within a secure key management scheme that may include any of the following: a) as cipher-text using a key which is appropriately secured; b) as encrypted key fragments using multiple control and split knowledge/ownership; or in another secure cryptographic module such as a key transportation device using multiple control.	
4.2.4	Backup copies of the CA's private keys are subject to the same or greater level of security controls as keys currently in use. The recovery of the CA's keys is carried out in as secure a manner as the backup process, using multi-person control.	
4.3	CA Public Key Distribution The CA maintains controls to provide reasonable assurance that the integrity and authenticity of the CA public keys and any associated parameters are maintained during initial and subsequent distribution.	
4.3.1	For the Root CA distribution process (e.g., using a self-signed certificate), an out-of-band notification mechanism is employed. Where a self-signed certificate is used for any CA, the CA provides a mechanism to verify the authenticity of the self-signed certificate (e.g., publication of the certificate's fingerprint). For Intermediate, Issuing, and/or Subordinate CA public keys these are validated by using a chaining method or similar process to link back to the trusted Root Certificate.	
4.3.2	The initial distribution mechanism for the CA's public key is controlled and initially distributed within a Certificate using one of the following methods: a) machine readable media (e.g., smart card, flash drive, CD ROM) from an authenticated source; b) embedding in an entity's cryptographic module; or other secure means that ensure authenticity and integrity.	
4.3.3	The CA's public key is changed (rekeyed) periodically according to the requirements of the CPS with advance notice provided to avoid disruption of the CA services.	
4.3.4	The subsequent distribution mechanism for the CA's public key is controlled in accordance with the CA's disclosed business practices.	
4.3.5	If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods: a) direct electronic transmission from the CA; b) placing into a remote cache or directory; c) loading into a cryptographic module; or any of the methods used for initial distribution.	

4.3.6	The CA provides a mechanism for validating the authenticity and integrity of the CA’s public keys.	
4.4	CA Key Usage The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations.	
4.4.1	The activation of the CA private signing key is performed using multi-party control (i.e., m of n) with a minimum value of m (e.g., m greater than 2 for Root CAs).	
4.4.2	If necessary based on a risk assessment, the activation of the CA private key is performed using multi-factor authentication (e.g., smart card and password, biometric and password, etc.).	
4.4.3	CA signing key(s) used for generating certificates and/or issuing revocation status information, are not used for any other purpose.	
4.4.4	The CA ceases to use a key pair at the end of the key pair’s defined operational lifetime or when the compromise of the private key is known or suspected.	
4.4.5	An annual review is required by the PA on key lengths to determine the appropriate key usage period with recommendations acted upon.	
4.5	CA Key Archival The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential, secured, and are never put back into production.	
4.5.1	Archived CA keys are subject to the same or greater level of security controls as keys currently in use.	
4.5.2	All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site.	
4.5.3	Archived keys are only accessed where historical evidence requires validation. Control processes are required to ensure the integrity of the CA systems and the key sets.	
4.5.4	Archived keys are recovered for the shortest possible time period technically permissible to meet business requirements.	
4.5.5	Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.	
4.6	CA Key Destruction The CA maintains controls to provide reasonable assurance that: • copies of CA keys that no longer serve a valid business purposes are destroyed in accordance with the CA’s disclosed business practices; and copies of CA keys are completely destroyed at the end of the key pair life cycle in accordance with the CA’s disclosed business practices.	
4.6.1	The CA’s private keys are not destroyed until the business purpose or application has ceased to have value or legal obligations have expired as disclosed within the CA’s CPS.	
4.6.2	Authorisation to destroy a CA private key and how the CA’s private key is destroyed (e.g., token surrender, token destruction, or key overwrite) are limited in accordance with the CA’s CPS.	
4.6.3	All copies and fragments of the CA’s private key are destroyed at the end of the key pair life cycle in a manner such that the private key cannot be retrieved.	
4.6.4	If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.	
4.6.5	If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device.	
4.6.6	If a CA cryptographic device case is intended to provide tamper-evident	

	characteristics and the device is being permanently removed from service, then the case is destroyed.	
4.6.7	Backup or additional copies of CA keys that no longer serve a valid business purpose are destroyed in accordance with the CA's disclosed business practices.	
4.6.8	The CA follows a CA key destruction script for key destruction ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key destruction ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed; d) specific steps performed during the key destruction ceremony, including; a. HSM and/or cryptographic hardware zeroisation/initialisation b. HSM and/or cryptographic hardware physical destruction c. Deletion of any encrypted files containing the CA key or fragments thereof e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the key destruction ceremony pending their disposal or additional destruction g) sign-off on the script or in a log from participants and witnesses indicating whether the key destruction ceremony was performed in accordance with the detailed key destruction ceremony script; and notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues).	
4.6.9	CA key destruction ceremonies are independently witnessed by internal or external auditors.	
4.7	CA Key Compromise The CA maintains controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the CA's private keys and any certificates, signed with the compromised keys, are revoked and reissued.	
4.7.1	The CA's business continuity plans address the compromise or suspected compromise of a CA's private keys as a disaster.	
4.7.2	Disaster recovery procedures include the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise of a CA's private signing key.	
4.7.3	The recovery procedures used if the CA's private key is compromised include the following actions: a) how secure key usage in the environment is re-established; b) how the CA's old public key is revoked; c) how affected parties are notified (e.g., impacted CAs, Repositories, Subscribers and CVSPs); d) how the CA's new public key is provided to the end entities and Relying Parties together with the mechanism for their authentication; and how the subscriber's public keys are re-certified.	
4.7.4	In the event that the CA has to replace its Root CA private key, procedures are in place for the secure and authenticated revocation of the following: a) the old CA root public key; b) the set of all certificates (including any self-signed) issued by a Root CA or any CA based on the compromised private key; and	

	any subordinate CA public keys and corresponding certificates that require recertification.	
4.7.5	The CA’s business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.	
4.7.6	The CA’s business continuity plan considers key replication techniques.	
4.8	CA Cryptographic Hardware Life Cycle Management The CA maintains controls to provide reasonable assurance that: • devices used for private key storage and recovery, and the interfaces to these devices are tested before usage for integrity; • access to CA cryptographic hardware is limited to authorised personnel in trusted roles, using multiple person control; and CA cryptographic hardware is functioning correctly.	
4.8.1	CA cryptographic hardware which does not contain CA keys is sent from the manufacturer or alternate CA site via registered mail (or equivalent) using tamper evident packaging. Upon the receipt of CA cryptographic hardware from the manufacturer or alternate site, authorised CA personnel inspects the tamper evident packaging to determine whether the seal is intact.	
4.8.2	Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed. Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.	
4.8.3	To prevent tampering, CA cryptographic hardware is stored and used in a secure site, with access limited to authorised personnel, having the following characteristics: a) inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; b) access control processes and procedures to limit physical access to authorised personnel; c) recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g., a safe) in audit logs; d) incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports; and monitoring processes and procedures to verify the ongoing effectiveness of the controls.	
4.8.4	When not attached to the CA system, the CA cryptographic hardware is stored in a tamper resistant container that is stored securely under multiple controls (i.e., a safe).	
4.8.5	The handling of CA cryptographic hardware, including the following tasks, is performed in the presence of no less than two trusted employees: a) installation of CA cryptographic hardware; b) removal of CA cryptographic hardware from production; c) servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware, or software); and disassembly and permanent removal from use.	
4.8.6	Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.	
4.8.7	Correct processing of CA cryptographic hardware is verified on a periodic basis.	

4.8.8	Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees.	
4.10	CA Key Transportation (if applicable) The CA maintains controls to provide reasonable assurance that: • CA private keys that are physically transported from one facility to another remain confidential and maintain their integrity; • CA hardware containing CA private keys, and associated activation materials, are prepared for transport in a physically secure environment (see §3.4) by authorised personnel in trusted roles, using multiple person controls, and are transported within sealed tamper evident packaging; • CA keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and • CA key transportation events are logged. *Explanatory Guidance:* CA Key Transportation refers to any event in which CA private signing keys are physically transported from one facility to another. This includes cases where the CA is migrating its production facility to another data centre, or when copies of the CA key are sent from the production facility to an alternate facility for backup or archive. It also includes situations in which the CA has acquired the CA keys from another entity, or has sold its CA keys to another entity. Activation materials refers to items including but not limited to passwords, PINs, tokens (i.e. m of n tokens) and/or key-wrapping keys needed to access and/or activate the CA key on the secure cryptographic module and must not be transported together with the CA keys. The intent of this criterion is for CA keys to maintain their confidentiality and integrity during transportation, and to be transported in a manner that prevents the keys from being activated or accessed during their transportation, including transporting associated activation materials separately. The methods to accomplish this vary based on the circumstances of how the CA keys are stored and protected. For example, some cryptographic hardware store keys directly within the device, whereas others store the key in an encrypted form on a client file system (i.e. on a hard disk) with the master key stored on a series of activation cards and utilise the cryptographic device to access the content of the client file system. Different considerations for transportation and security will need to be applied in both of those examples.	
4.10.1	CA keys are prepared for transport in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control.	
4.10.2	CA keys remain in a physically secure environment (see §3.4) until ready to be transported by CA personnel or common carrier.	
4.10.3	CA keys are only transported on hardware devices and in tamper-evident packaging as disclosed in the CA's business practices.	
4.10.4	If the hardware device contains the entire CA key, it is physically transported by at least two CA employees and remains under multi-person control from origin to destination.	
4.10.5	If the CA key is divided into fragments on multiple hardware devices: a) If transported by CA employees, each fragment is transported separately using different transportation routes, methods, and/or times; or If transported by common carrier, each fragment is sent using a different common carrier at different times. Shipments require signature service, tracking, are insured.	

4.10.6	Activation materials are transported separately from the CA key (i.e. by a different method and/or at a different time) in tamper-evident packaging.	
4.10.7	Upon receipt at the destination, packaging for CA keys and activation materials are reviewed for evidence of tampering. If evidence of tampering is discovered, the Policy Authority is notified of a possible breach event.	
4.10.8	Upon receipt at the destination, CA keys and activation materials are stored in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control.	
4.10.9	Personnel involved in a CA key transportation event are in Trusted Roles and have received training in their role and responsibilities.	
4.10.10	A log is maintained of all actions taken as part of the CA key transportation event and is retained in accordance with the CA's disclosed business practices.	
4.10.11	Internal or external auditors accompany CA personnel during CA key transportation events.	
4.11	CA Key Migration (if applicable) The CA maintains controls to provide reasonable assurance that: • CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration (see §4.2), are completed in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control; • hardware and software tools used during the CA key migration process are tested by the CA prior to the migration event; and • CA key migration events follow a documented script and are logged. *Explanatory Guidance:* CA Key Migration refers to events in which the CA is migrating its private signing keys from one secure cryptographic device to another. For example, this would encompass instances where the CA is upgrading from an older device model to a newer model, switching to a different hardware vendor, or migrating keys it acquired from another entity onto its own infrastructure. Routine backup and restorations (for example, transferring keys from a primary network hardware security module to a backup hardware security module token) when performed using approved methods from the hardware vendor are covered by Criterion 4.2. All other key movements between hardware devices are addressed by this Criterion 4.11.	
4.11.1	CA key migration events occur in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control.	
4.11.2	Vendor-supplied hardware and software tools are tested by the CA prior the key migration event, and are operated in accordance with vendor-supplied documentation and instructions.	
4.11.3	In-house developed software tools are developed and tested by the CA prior to the key migration event in accordance with its standard software development process (see §3.7).	
4.11.4	The CA follows a CA key migration script for key migration events that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key migration event c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be migrated and new hardware where the keys are being migrated to; d) specific steps performed during the key migration ceremony, including; • Hardware preparation • Software tool installation and setup • Cryptographic hardware setup and initialisation	

	- CA key migration - CA key verification e) physical security requirements for the event location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the migration event g) sign-off on the script or in a log from participants and witnesses indicating whether the key migration was performed in accordance with the detailed key migration script; and notation of any deviations from the key migration script (e.g., documentation of steps taken to address any technical issues).	
4.11.5	A log is maintained of all actions taken as part of the CA key migration event and is retained in accordance with the CA's disclosed business practices.	
4.11.6	CA key migration events are witnessed by internal or external auditors.	
4.11.7	Upon successful completion of a CA key migration event, remaining copies of the CA keys, and older cryptographic hardware that no longer serve a business purpose are securely destroyed in accordance with the CA's disclosed business practices (see §4.5).	
6.0	**Certificate Lifecycle Management** The Certification Authority maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated (for the registration activities performed by ABC- CA).	
6.1	Subscriber Registration The CA maintains controls to provide reasonable assurance that: For authenticated certificates - subscribers are accurately identified in accordance with the CA's disclosed business practices; - subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and - subscribers' certificate requests are accurate, authorised and complete. for domain validated certificates - Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and - Subscriber's certificate requests are accurate and complete.	

6.1.1	For authenticated certificates, the CA verifies or requires that the RA verify the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements of the CP. a) For individual end entity certificates, the CA or RA verifies the identity of the person whose name is to be included in the subscriber distinguished name field of the certificate. An unauthenticated individual name is not included in the subscriber distinguished name. *b)* For organisational certificates (including role based, server, network resource, code signing, etc.), the CA or RA verifies the legal existence of the organisation's name and the authority of the requesting party to be included in the organisation attribute in the subscriber distinguished name field of the certificate. An unauthenticated organisation name is not included in a certificate. c) For organisational certificates containing a domain name of an organisation, the CA or RA verifies the organisation's ownership, control, or right to use the domain name and the authority of the requesting party included in the common name attribute of the subscriber distinguished name field of the certificate. An unauthenticated domain name is not included in a certificate.	
6.1.2	For domain and/or IP address validated certificates, the CA validates or requires that the RA validate (as determined by the CP) the organisation's ownership, control, or right to use the domain name and/or IP address.	
6.1.3	The CA or RA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the CP.	
6.1.4	The CA or RA checks the Certificate Request for errors or omissions in accordance with the CP.	
6.1.5	For end entity certificates, the CA uses the RA's public key contained in the requesting entity's Certificate Request to verify signature on the Certificate Request submission.	
6.1.6	The CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP.	
6.1.7	Encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.	
6.1.8	At the point of registration (before certificate issuance) the RA or CA informs the Subscriber of the terms and conditions regarding use of the certificate.	
6.1.9	Before certificate issuance, the CA informs the Subscriber of the terms and conditions regarding use of the certificate.	
6.1.10	The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (Registration Request) to an RA (or the CA) as specified in the CP.	
6.1.11	The CA requires that the requesting entity submit its public key in a self-signed message to the CA for certification. The CA requires that the requesting entity digitally sign the Registration Request using the private key that relates to the public key contained in the Registration Request in order to: a) allow the detection of errors in the certificate application process; and b) prove possession of the companion private key for the public key being registered.	
6.1.12	The certificate request is treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the Subscriber Agreement.	
6.1.13	The CA validates the identity of the RA authorised to issue registration requests under a specific CP.	

6.1.14	The CA requires that RAs submit the requesting entity’s certificate request data to the CA in a message (Certificate Request) signed by the RA. The CA verifies the RA’s signature on the Certificate Request.	
6.1.15	The CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility in accordance with the CA’s CPS.	
6.1.16	The CA requires that RAs record their actions in an audit log.	
6.1.17	The CA verifies the authenticity of the submission by the RA in accordance with the CA’s CPS.	
6.2	Certificate Renewal (if supported) The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorised and complete. *Explanatory Guidance: Certificate Renewal is the process in which a subscriber can obtain a new certificate to replace an old certificate that:* • *Contains the same information (identity, domains, etc.) as the old certificate* • *Has a new validity period ending after the validity period of the old certificate* • *Contains the same public key as the old certificate* If CA does not have controls in place to prevent a subscriber from using the same key pair to request a certificate that has the same information as a previously-issued and valid certificate, then it de facto supports Certificate Renewal, even if not explicitly stated.	
6.2.1	The Certificate Renewal Request includes at least the subscriber’s Distinguished Name, the Serial Number of the certificate (or other information th0 at identifies the certificate), and the requested validity period. (The CA will only renew certificates that were issued by itself.)	
6.2.2	The CA requires that the requesting entity digitally sign the Certificate Renewal Request using the private key that relates to the public key contained in the requesting entity’s existing public key certificate.	
6.2.3	The CA issues a new certificate using the subscriber’s previously certified public key, only if its cryptographic security is still sufficient for the new certificate’s intended lifetime and no indications exist that the subscriber’s private key has been compromised.	
6.2.4	For renewal of authenticated certificates, the CA or the RA process the certificate renewal data to verify the identity of the requesting entity and to identify the certificate to be renewed.	
6.2.5	For domain validated certificates, the CA or the RA process the certificate renewal data to re-validate the domain in accordance with the requirements of the CP.	
6.2.6	The CA or the RA validate the signature on the Certificate Renewal Request.	
6.2.7	The CA verifies the existence and validity of the certificate to be renewed. The CA does not renew certificates that have been revoked, expired or suspended.	
6.2.8	The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements defined in the CP.	
6.2.9	The CA requires that RAs submit the Certificate Renewal Data to the CA in a message (Certificate Renewal Request) signed by the RA.	
6.2.10	The CA requires that the RA secures that part of the certificate renewal process for which it (the RA) assumes responsibility in accordance with the CP.	
6.2.11	The CA requires that RAs record their actions in an audit log.	
6.2.12	The CA verifies the authenticity of the submission by the RA.	
6.2.13	The CA verifies the RA’s signature on the Certificate Renewal Request.	
6.2.14	The CA checks the Certificate Renewal Request for errors or omissions. This function may be delegated explicitly to the RA.	

6.2.15	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP.	
6.2.16	The CA issues a signed notification indicating the certificate renewal has been successful.	
6.2.17	The CA makes the new certificate available to the end entity in accordance with the CP.	
6.3	Certificate Rekey The CA maintains controls to provide reasonable assurance that certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorised and complete. *Explanatory Guidance: Certificate Rekey is the process in which a subscriber can obtain a new certificate to replace an old certificate that:* • *Contains the same information (identity, domains, etc.) as the old certificate* • *Has the same expiry date (notAfter date) as the old certificate* • *Contains a different public key as the old certificate* In some cases, a CA may refer to Certificate Rekey as a ‘renewal’, however, if the process results in the subscriber having a new certificate issued with a different public key (whether voluntary on the part of the subscriber or mandated by the CA), then this is a Certificate Rekey. A Certificate Renewal only occurs when the same key pair is recertified (see §6.2)	
6.3.1	A Certificate Rekey Request includes at least the subscriber’s distinguished name, the serial number of the certificate, and the requested validity period to allow the CA or the RA to identify the certificate to rekey.	
6.3.2	The CA requires that the requesting entity digitally sign, using the existing private key, the Certificate Rekey Request containing the new public key.	
6.3.3	For authenticated certificates, the CA or the RA processes the Certificate Rekey Request to verify the identity of the requesting entity and identify the certificate to be rekeyed.	
6.3.4	For domain validated certificates, the CA or the RA process the Certificate Rekey Request to re-validate the domain in accordance with the requirements of the CP.	
6.3.5	The CA or the RA validates the signature on the Certificate Rekey Request.	
6.3.6	The CA or the RA verifies the existence and validity of the certificate to be rekeyed.	
6.3.7	The CA or the RA verifies that the Certificate Rekey Request meets the requirements defined in the relevant CP.	
6.3.12	The CA or the RA checks the Certificate Rekey Request for errors or omissions.	
6.3.13	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for rekey.	
6.3.14	Prior to the generation and issuance of rekeyed certificates, the CA or RA verifies the following: a) the signature on the certificate rekey data submission; b) the existence and validity supporting the rekey request; and c) that the request meets the requirements defined in the CP.	
6.4	Certificate Issuance The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA’s disclosed business practices.	

6.4.1	The CA generates certificates using Certificate Request Data and manufactures the certificate as defined by the appropriate Certificate Profile in accordance with ISO 9594/X.509 and ISO 15782-1 formatting rules as disclosed within the CP.	
6.4.2	Validity periods are set in the CP and are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.	
6.4.3	Extension fields are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.	
6.4.4	The CA signs the end entity's public key and other relevant information with the CA's private signing key.	
6.4.5	The CA publishes the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices.	
6.4.6	When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.	
6.4.7	Certificates are issued based on approved subscriber registration, certificate renewal or certificate rekey requests in accordance with the CP.	
6.4.8	The CA issues a signed notification to the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.	
6.4.9	The CA issues an out-of-band notification to the Subscriber when a certificate is issued. Where this notification includes initial activation data, then control processes ensure safe delivery to the Subscriber.	
6.4.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time specified in the CP.	
6.5	Certificate Distribution The CA maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.	
6.5.1	The CA makes the certificates issued by the CA available to relevant parties using an established mechanism (e.g., a repository such as a directory) in accordance with the CP.	
6.5.2	Only authorised CA personnel administer the CA's repository or alternative distribution mechanism.	
6.5.3	The performance of the CA's repository or alternative distribution mechanism is monitored and managed.	
6.5.4	The integrity of the repository or alternative distribution mechanism is maintained and administered.	
6.5.5	Where required under privacy legislation, certificates are made available for retrieval only in those cases for which the subscriber's consent is obtained.	
6.6	Certificate Revocation The CA maintains controls to provide reasonable assurance that certificates are revoked, based on authorised and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.	
6.6.1	The CA provides a means of rapid communication to facilitate the secure and authenticated revocation of the following: a) one or more certificates of one or more subscribers; b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c) all certificates issued by a CA, regardless of the public/private key pair used.	

6.6.2	The CA verifies or requires that the RA verify the identity and authority of the entity requesting revocation of a certificate in accordance with the CP.	
6.6.5	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms in the timeframes specified within the CP and in accordance with the format defined in ISO 9594/X.509 and ISO 15782-1.	
6.6.6	The CA records all certificate revocation requests and their outcome in an audit log.	
6.6.7	The CA or RA may provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.	
6.6.8	Where certificate renewal is supported, when a certificate is revoked, all valid instances of the certificate are also revoked and are not reinstated.	
6.6.9	The Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate.	
6.7	Certificate Suspension (if supported) The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorised and validated certificate suspension requests within the time frame in accordance with the CA’s disclosed business practices. *Explanatory Guidance: Certificate Suspension is the process in which a certificate is effectively revoked for a ‘temporary’ period of time. Unlike revocation which is ‘permanent’ and can only be ‘undone’ by issuing a new certificate, suspension allows the certificate to be reinstated at a later period of time. During the time a certificate is suspended, it will appear on revocation lists, typically with a status of ‘Certificate Hold’. CAs may only support Certificate Suspension for certain types of certificates.*	
6.7.1	The CA provides a means of rapid communication to facilitate the secure and authenticated suspension of the following: a) one or more certificates of one or more subscribers; b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c) all certificates issued by a CA, regardless of the public/private key pair used.	
6.7.4	The CA or RA notifies the Subscriber in the event of a certificate suspension.	
6.7.5	Certificate suspension requests are processed and validated in accordance with the requirements of the CP.	
6.7.6	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status are completed in a time frame determined by the CP.	
6.7.7	Certificates are suspended only for the allowable length of time in accordance with the CP.	
6.7.8	Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways: a) an entry for the suspended certificate remains on the CRL with no further action; b) the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate; or c) the suspended certificate is explicitly released and the entry removed from the CRL.	
6.7.9	A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.	
6.7.10	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with the CA’s CP.	

6.7.12	Certificate suspensions and the lifting of certificate suspensions are recorded in an audit log.	
6.8	Certificate Validation The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms) is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.	
6.8.1	The CA makes certificate status information available to relevant entities (Relying Parties or their agents) using an established mechanism in accordance with the CP. This is achieved using: a) Request Response Method – A request signed by the Relying Party to the Certificate Status Provider's responder. In turn, the Certificate Status Provider's responder responds with the certificate status duly signed. (OCSP is an example protocol using this method.) b) Delivery Method – A CRL signed by the CA and published within the policy's time frame.	
6.8.2	The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date and time of issuance.	
6.8.3	The CA issues CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance.	
6.8.4	At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period.	
6.8.5	If certificate suspension is supported, a certificate suspension (hold) entry, with its original action date and expiration date remain on the CRL until the normal expiration of the certificate or until the suspension is lifted.	
6.8.6	CRLs are archived in accordance with the requirements of the CP including the method of retrieval.	
6.8.7	CAs include a monotonically increasing sequence number for each CRL issued by that CA.	
6.8.8	The CRL contains entries for all revoked unexpired certificates issued by the CA.	
6.8.9	Old CRLs are retained for the appropriate period of time specified in the CA's CP.	
6.8.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time as disclosed in the CP.	
6.8.11	If an online certificate status collection method (e.g., OCSP) is used, the CA requires that certificate status inquiries (e.g., OCSP requests) contain all required data in accordance with the CP.	

6.8.12	Upon the receipt of a certificate status request (e.g., an OCSP request) from a Relying Party or its agent, the CA returns a definitive response to the Relying Party or its agent if: a) the request message is well formed; b) the Certificate Status Provider responder is configured to provide the requested service; c) the request contains the information (i.e., certificate identity – Serial number, OID, etc.) needed by the Certificate Status Provider responder in accordance with the CP; and d) the Certificate Status Provider's responder is able to locate the certificate and interpret its status. Where these conditions are met, the CA or Certificate Status Provider produces a signed response message indicating the certificate's status in accordance with the CP. If any of the above conditions are not met then a status of unknown may be returned.	
6.8.13	All response messages are digitally signed and include all required data in accordance with the CP.	
7.0	7.0: Subordinate CA - Lifecycle Management Controls The Certification Authority maintains effective controls to provide reasonable assurance that subordinate CA certificate - requests are accurate, authenticated and approved.	
7.1	Subordinate CA Certificate - Lifecycle Management The CA maintains controls to provide reasonable assurance that: • subordinate CA - requests are accurate, authenticated and approved; • subordinate CA - replacement (renewal and rekey) requests are accurate, authorised, complete; • new, renewed and rekeyed Subordinate CA are generated and issued in accordance with the CA's disclosed business practices; • upon issuance, complete and accurate Subordinate CA - are available to relevant entities (Subscribers and Relying Parties) in accordance with the CA's disclosed business practices; • subordinate CA are revoked based on authorised and validated certificate revocation requests; and • timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA's disclosed business practices. *Explanatory Guidance: A Subordinate CA certificate is a CA certificate issued by the Parent CA (typically using a Root CA) to a non-affiliated subordinate CA, typically to be operated under the Parent CA's CP.*	
7.1.1	The Parent CP specifies the requirements for submission of Sub-CA requests.	
7.1.2	The Parent CA authenticates the Sub-CA request in accordance with the Parent's CP.	
7.1.3	The Parent CA performs an assessment of the Sub-CA - applicant's compliance with the requirements of the Parent CA's CP before approving a Sub-CA - request, or alternatively the Sub-CA - applicant presents its CPS for assessment.	
7.1.4	Where Sub-CA renewal is permitted, the Parent CA's CP specifies the requirements for submission of Sub-CA - renewal requests.	
7.1.5	Where Sub-CA certificate - renewal is permitted, the Parent CA authenticates the Sub-CA - renewal request in accordance with the CA's CP.	

7.1.4	Where Sub-CA - renewal is permitted, the Parent CA’s CP specifies the requirements for submission of Sub-CA - renewal requests.	
7.1.5	Where Sub-CA certificate - renewal is permitted, the Parent CA authenticates the Sub-CA - renewal request in accordance with the CA’s CP.	
7.1.6	The Parent CA’s CP specifies the requirements for submission of Sub-CA rekey requests.	
7.1.7	The Parent CA authenticates the Sub-CA certificate rekey request in accordance with the CP.	
7.1.8	The Parent CA generates certificates: a) using the appropriate certificate profile in accordance with the CP and ISO 9594/X.509 and ISO 15782-1 formatting rules; b) with the validity periods formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP; and where extensions are used, with extension fields formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP.	
7.1.9	The Parent CA signs the Sub-CA - with the Parent CA's private signing key.	
7.1.10	The Parent CA makes Sub-CA - available to relevant entities (e.g., Relying Parties) using an established mechanism (e.g., a repository such as a directory) in accordance with the Parent CA’s CP.	
7.1.11	The Parent CA verifies the identity and authority of the entity requesting revocation of a Sub-CA - in accordance with the Parent CA’s CP.	
7.1.12	The Parent CA updates the Certificate Revocation List (CRL) and other Sub-CA status mechanisms upon certificate revocation in accordance with the Parent CA’s CP.	
7.1.13	The Parent CA makes Sub-CA - status information available to Relying Parties using an established mechanism (e.g., CRL, OCSP, etc.) in accordance with the Parent CA’s CP.	

***