National Internet Exchange of India

Request for Proposal (RFP) For Setting of SSL Roots setup along with SSL of CA facility at NIXI
RFP No: CCA/01(1)-2022-NIXI
Ref: F.No.NIXI/CCA/01-2022 Dated 11/10/2022

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
1	Schedule for Invitation of RFP	2	Proposal Submission End Date/Time: 26-10-2022 @ 15:00 hrs.	In view of the size and complexity of the RFP requirement and the upcoming holidays for the festivities we would request NIXI to extend the bid submission date by at least 30 days from the date of publication of the corrigendum in response to the pre-bid queries so that all probable bidders can get sufficient time to study the RFP and prepare a comprehensive tender response which would address the requirement of CCA.	Date extended till 4th Nov, 2022.
2	3. Eligibility Criteria for Participation in this Tender:	9	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.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request NIXI to kindly consider the relevant documentary evidence of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	NO changes.
3	3. Eligibility Criteria for Participation in this Tender:	9, 10	2. The Bidder shall have revenue of INR 100 crs and shall be profitable for the last 3 financial years (FY 2021-22, 20-21, 19-20). The evidences shall be provided.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request NIXI to kindly consider the audited financial statements of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	The clause is self expalanary.
4	Eligibility criteria for OEM (PKI Software):	11	5. The OEM shall have experience in establishing atleast one WebTrust Accredited CA.	As the WebTrust Accreditation for a CA is a relatively new requirement, it will severely limit the number of vendors who can participate in the RFP and hence the options available to NIXI will be less. In view of the above and to promote wider participation we would request NIXI to kindly remove this criteria.	NO changes.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
5	Eligibility criteria for OEM (PKI Software):	12	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 3 Root CA's in Asia	We would request NIXI for relaxation for this RFP requirement as OEMs/ Vendors based out of India catering to Indian CA's will have challenges to meet this requirement, once again limiting the number of vendors who can participate.	NO changes.
6	Eligibility criteria for OEM (PKI Software):	12	8. OEM should be actively participating in international policy making bodies / committees like CAB Forum, WebTrust, IETF etc.	To promote wider participation we would request NIXI for suitable relaxation for this RFP requirement as OEMs / Vendors based out of India catering to Indian CA's will have challenges to meet this requirement, once again limiting the number of Companies who can participate.	NO changes.
7	5. Pre-bid Meeting:	12	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)	Please confirm the date, time and venue for the Pre-Bid Meeting.	Response are being uploaded.
8	8.1.6 Technical bid	25	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.	As per page 2, we understand that EMD of Rs. 20 Lakh has to be deposited as bid security. So please clarify if the bidder has to deposit the EMD along with the " Bid Securing Declaration (BSD)".	EMD is indicated as mentioned in the RFP
9	6 Scope of work and Technical Specifications	45, 46	5. THE OFFERED SOLUTION SHOULD INCLUDE THE FOLLOWING: Equipment's required for smooth running an operation for CCA root and CA for SSL Fire Detection System- Smoke Detector, VESDA Fire Suppression System- FM 200 Fire extinguishers CCTV Biometric Access Control (Dual Factor) Water leakage Detector Passive Infrared Sensor Vibration Sensor Rodent Repellents Manned Security Dual Precision AC Dual UPS Emergency Response Team FRFC (2Nos) Safe Locker (6 Nos)	We would request NIXI to kindly provide the minimum technical specifications of the below listed solution components: Equipment's required for smooth running an operation for CCA root and CA for SSL Fire Detection System- Smoke Detector, VESDA Fire Suppression System- FM 200 Fire extinguishers CCTV Biometric Access Control (Dual Factor) Water leakage Detector Passive Infrared Sensor Vibration Sensor Rodent Repellents Manned Security Dual Precision AC Dual UPS Emergency Response Team FRFC (2Nos) Safe Locker (6 Nos)	The requiremst will be as WebTrust requirement.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
10	5. The payment terms are:	55, 56	b. Payment will be made as mentioned below: Complete Delivery, Installation, Commissioning and acceptance per site: 70 % value of contract price pertaining to equipment(s) at individual site d. 15% value of the total value of installed & accepted items shall be released after Submission of the all the documents to WebTrust. e. NIXI may give an option to contractor to claim Balance 15% payment against submission of Bank Guarantee after all the documentations as per WebTrust. However, if the vendor fails to get WebTrust in next 1 year after submission of all the documents, Bank Guarantee submitted will be encashed. Bank Guarantee formats and required undertaking to be signed by the contractor in this respect will be given to contractor at the time of exercising this option.	We would request NIXI to amend the Payment Terms as suggested below to align with the widely accepted payment schedule for similar projects: On Delivery at respective site - 70 % value of contract price pertaining to equipment(s) at individual site On Installation, Commissioning and Acceptance per site: 20 % value of contract price pertaining to equipment(s) at individual site Balance 10% value of the total value of installed & accepted items shall be released after Submission of the all the documents to WebTrust.	No change.
11	5. The payment terms are:	56	h. Manpower Warranty & Maintenance of Remote Sites will be released on quarterly basis after completion of each quarter from the start of services. 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 principle employer shall be liable to ensure compliance with all the applicable laws pertaining to the Manpower deployed.	We would request NIXI to suitably amend the Payment Terms for the AMC / ATS of the supplied hardware and software and make provision to process the AMC / ATS related payment annually in advance. Please confirm the acceptance of our request.	No change
12	12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default	59	5) Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause.	We would request NIXI to kindly drop the option to exercise the "Risk-and-Cost Procurement" clause and limit the remedies to forfeiture of PBG and termination of the Contract after issuing notice and providing sufficient time to undertake remedial actions. Please confirm the acceptance of our request.	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
13	Form4.1: Experience Statement	109	Statement of completion of Project Last five Years	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request NIXI to kindly consider the documentary evidence of the relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for RFP compliance. Please confirm the acceptance of our request.	The claus is elf expalanry.
14	8.1.6 Technical bid	25	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 Sal and End of Support. If the equipment is end of support in the next 5 years, OEM will declare that they will support the equipment for at least next 5+2=7 Years from original date of Installation and Commissioning. OEM Shall declare these in the Letter Head.	We would request NIXI to kindly amend the clause as suggested below: *Also, the OEM should declare that the equipment is not end of Sale and End of Support. If the equipment is end of support in the next 5 years, OEM will declare that they will support the equipment for at least next 5+2=7 Years from date of bid submission. OEM Shall declare these in the Letter Head.*	May be accpted as requested.
15	6 Scope of work and Technical Specifications	45	5. THE OFFERED SOLUTION SHOULD INCLUDE THE FOLLOWING:	Please include the details of the required components in the commercial bid format and BOQ section.	
16	6 Scope of work and Technical Specifications	45	Offering the state-of-art bill of material including hardware, operating software, application software (including various modules as per operational requirement of RCAI), access control system, CCTV, etc with exact make & model, even if some of the items are missing in the Bill of Material in the Tender Document.	We understand that the bidder is only responsible for the scope mentioned in the commercial format / BOQ section of the RFP. Please confirm.	Requiremennt is complete dnad if the bidder wants something to be added on esstial ground for WbTrust, may do so by addding a line item.
17	11 Acceptance Testing (AT):	47	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.	Please clarify if bidder has to provide the necessary networking links as part of scope.	New Link not to be established. However, the link to be configured as per the WebTrust requitrement.
18	11 Acceptance Testing (AT):	47	iii. Successful Vulnerability assessment (VA) and Penetration Testing (PT) report.	Please confirm if the Bidder is responsible for conducting VA and PT or NIXI shall get it done on their own. Kindly clarify.	Bidder will get it conducted as per requirement.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
19	6.2 Warranty and Maintenance:	49	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 for Three (3) year. The warranty period shall start from the date of successful commissioning by contractor and acceptance by NIXI for each site	As per prevalent practice of industry, the Warranty of each item starts from date of supply from OEM. There can be delay from NIXI side for site readiness, inputs, approval and acceptance. We request you to amend this clause as suggested herewith: *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 for Three (3) years. The warranty period shall start from the date of supply by Contractor or 3 years 6 months from date of purchase order, whichever is later.*	NO changes.
20	6.2 Warranty and Maintenance:	49	2) Warranty for those equipment(s) which will be delivered at Location -18 will start from the date of verification and successful power on test.	As per prevalent practice of industry, the Warranty of each item starts from date of supply from OEM. There can be delay from NIXI side for site readiness, inputs, approval and acceptance. We request you to amend this clause as suggested herewith: *2) Warranty for those equipment(s) which will be delivered at Location -18 will start from the date of supply by contractor or 3 years 8 months from date of purchase order, whichever is later.*	NO changes.
21	6.2 Warranty and Maintenance:	49	6) 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.	We understand Data Backup software has to be supplied by Bidder as part of this RFP scope as given in BOQ. Please confirm if the Bidder has to supply, install and configure data backup storage, backup server(s), Tape library, tape media etc. also as part of the scope of work. Further, please provide the data retention policy to size / estimate the backup infrastructure that would be required for project implementation.	Yes, the clause is self expalanary
22	6.2 Warranty and Maintenance:	49	8) All ongoing software upgrades for all major and minor releases should be provided during the warranty period	We understand that this clause is not applicable on underlying software such as Operating System(s) and Database(s) etc. Please confirm.	Yes, the clause is self expalanary

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
23	6.2 Warranty and Maintenance:	49	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. 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). The Resident Engineer as asked in the tender should be on direct muster-roll (pay-roll) of the Contractor.	(1) We understand that required resident engineer has to be deputed by Bidder as mentioned in Manpower Distributions (Year Wise). Please confirm. (2) We would request NIXI to kindly confirm the count of resident support engineers required for deployment.	Yes, the clause is self expalanary
24	9.4 Terms of Delivery installation, commissioning	53	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.	In the current global situation of post-pandemic, semiconductor shortage, and Russia-Ukraine war, the global supply chain is badly affected and delivery timelines cannot be met by any supplier / OEM for the items listed in BOQ as specified in this clause. In view of above, kindly provide requested delivery timelines to the bidder. We request for the necessary amendment of this clause as suggested herewith: *5. Contractor shall complete the delivery, installation, testing and commissioning of all the equipment(s) at all sites within* ***210 days*** *from the date of issuance of Contract.*	Yes, the clause is self expalanary .

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
25	9.6 Extension of Delivery Period and Liquidated Damages:	53	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 @ 1% 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.	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) of respective equipment at non-commissioned sites per week or part of the week of delayed period. Liquidated Damages shall not exceed 5% of the total contract value of respective equipment. In case, delay beyond 10 weeks, NIXI may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.	No change in clause
26	10 Prices and Payments Terms	55	c. Insurance Certificate/policy duly assigned in favour of O/o NIXI. (In case payment is claimed by Contractor within 60 days from the date of acceptance.)	We understand material insurance shall be taken care by NIXI post delivery at site. Please confirm	The terms are self explanary
27	Complete List of BoQ	61	Database	Please provide database details and core(s) to be licensed	Bidder will provide the itesm as per WebTrust requirement.
28	Complete List of BoQ	61	LogServer	Please provide minimum specifications of Log servers	Bidder will provide the itesm as per WebTrust requirement.
29	Complete List of BoQ	61	Back Up Software	Please provide how much TB or sockets to be license to be supplied by bidder.	Bidder will provide the itesm as per WebTrust requirement.
30	Complete List of BoQ	61	Active Directory	Please confirm no of AD licenses to be supplied by bidder. Also confirm if underline server and operating system etc. are to be supplied by bidder to run the AD solution.	Bidder will provide the itesm as per WebTrust requirement.
31	Complete List of BoQ	61	Mail Server	Please provide minimum specifications of mail server. Also confirm, if bidder has to supply, configure and migrate any mail solution on these servers.	Bidder will provide the itesm as per WebTrust requirement.
32	Complete List of BoQ	61	Operating System	Please provide version and number of core/sockets to be licensed.	Bidder will provide the itesm as per WebTrust requirement.
33	Complete List of BoQ	62	Tape Drive	Please provide specification and LTO type of tape drive including number of drives required.	Bidder will provide the itesm as per WebTrust requirement.
34	Complete List of BoQ	62	Tape	This refer to Tape Data Cartridge. Please confirm	Bidder will provide the itesm as per WebTrust requirement.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
35	Specifications for Servers	75	Physical specifications	We would request NIXI to kindly remove the speciation table as requisite servers specifications supply and solution availability is Bidder's responsibility. These specifications looks very detailed and difficult for bidder to find a qualified server OEM with these specifications which meets the RFP requirement.	Bidder will provide the itesm as per WebTrust requirement.
36	Specifications for Fiber Transmission 19” Smart Rack	80	Specifications for Fiber Transmission 19” Smart Rack	This item is not part of BOQ. Would request NIXI to include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence request NIXI to relax the same so that other competent OEMs can also comply with the same.	It is part of the Price bid and bidder need to add the line item.
37	Specifications of Web Application Firewall	81	Specifications of Web Application Firewall	This item is not part of BOQ. Would request NIXI to include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence request NIXI to relax the same so that other competent OEMs can also comply with the same.	Bidder will provide the itesm as per WebTrust requirement.
38	Data Leakage Prevention	82	Data Leakage Prevention	This item is not part of BOQ. Would request NIXI to include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence request NIXI to relax the same so that other competent OEMs can also comply with the same.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever.
39	Technical Specifications of Load Balancer	87	Technical Specifications of Load Balancer	This item is not part of BOQ. Would request NIXI to include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence request NIXI to relax the same so that other competent OEMs can also comply with the same.	Bidder will provide the items as per WebTrust requirement and to be added as Line items for the same.
40	For the full Duplex Should have the Following specifications	89	For the full Duplex Should have the Following specifications	We would request NIXI to kindly delete these specification and allow Bidder to supply switches as per their solution requirements.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
41	Technical Specifications SAN Storage - Specifications	89	Technical Specifications SAN Storage - Specifications	This item is not part of BOQ. Requesting NIXI to kindly include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence we would request NIXI to kindly delete the same so that Bidder can supply as per their solution requirements.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever. It will be as pert of the Commercial Bid and BOF.
42	Technical Specifications for Multiservice Switch	92	Technical Specifications for Multiservice Switch	This item is not part of BOQ. Requesting NIXI to kindly include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence we would request NIXI to kindly delete the same so that Bidder can supply as per their solution requirements.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever and may delete any restrictive clause. The Tender evaluation Committee will do due diligence if required.
43	Technical Specifications for Firewall	92	Technical Specifications for Firewall	This item is not part of BOQ. Requesting NIXI to kindly include the same in BOQ with its quantity, if its in Bidder's scope of supply and installation. These specifications also looks OEM specific, hence we would request NIXI to kindly delete the same so that Bidder can supply as per their solution requirements.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever and may delete any restrictive clause. The Tender evaluation Committee will do due diligence if required.
44	Form 1.3: OEM's Authorization	102	Form 1.3: OEM's Authorization	As per industry standard, all OEMs provide the MAF in their own internal Legal Cell approved template. So, we would request NIXI to kindly accept the OEM standard MAF.	Bidder will provide the items as per WebTrust requirement. NIXI is not for of any propreity specific product whatso ever and may delete any restrictive clause. The Tender evaluation Committee will do due diligence if required.
45	General		General Query	We understand NIXI will provide the necessary data center services required for the implementation of the project such as rack space, appropriate power sockets, cooling, security components, network, virtualisation, access, storage space, connectivity, links, Internet, sitting space etc. Please confirm our understanding.	The clause is self explanary and may accordingly submit their bids.
46	General		Exchange Rate Variation	Given the volatility in foreign exchange rates, we request NIXI to kindly include an **Exchange Rate Variation Protection Clause** to safeguard the Bidders from exchange rate fluctuations.	No change.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
47	Section I: Notice Inviting Tender (NIT) -> 3.Eligibility Criteria for Participation in this Tender -> Point 2	10	Not have a conflict of interest, which substantially affects fair competition.	Please explain / define what constitutes conflict of interest for a bidder while submitting proposal.	The clause is self explianary.
48	Section I: Notice Inviting Tender (NIT) -> 3.Eligibility Criteria for Participation in this Tender -> Point 4 Pg. No. 10	10	The Bidder shall select the OEM with appropriate knowledge, experience and expertise in setting up, managing the CA infrastructure and have expertise in handling WebTrust accreditation program.	This is the first WebTrust requirement in India and for wider participation of OEMs, we request NIXI to consider relaxing the WebTrust accreditation requirement for the OEM.	No change.
49	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 5 Pg. No. 11	11	The OEM shall have experience in establishing atleast one WebTrust Accredited CA.	This is the first WebTrust requirement in India and for wider participation of OEMs, we request NIXI to consider relaxing the WebTrust accreditation requirement for the OEM. It may be instead mandated to the Bidder to include a WebTrust empanelled auditor in the engagement.	No change
50	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 1 Pg. No. 11	11	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.	The proposed CA solution is deployed across various Certifying Authorities and has also been audited by CCA empanelled auditors at many instances. Considering this and for wider participation in the tender we urge NIXI to relax this clause.	No change
51	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 7 Pg. No. 12	12	OEM should have supplied & successfully implemented Certificate Authority and OCSP solution during the last 03 (Three) years till 31st March 2022 in at least 3 Root CA's in Asia	Please clarify whether this criteria is for deployment of CA/OCSP solution for 3 Certifying Authorities (or) 3 Root Certifying Authority of a Country. If it is for RCAI deployment, to enable various OEMs to participate, we request NIXI to modify the clause to show evidences of 3 deployments for Certifying Authorities in Asia	No change.
52	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 8 Pg. No. 12	12	OEM should be actively participating in international policy making bodies/ committees like CAB Forum, WebTrust, IETF etc.	Compliance of Software stack and infrastructure to WebTrust and CAB forum guidelines should be the requirement rather than participation in the forum / Body. Hence we request NIXI to relax this clause.	No change
53	Section II: Instructions to	16	Root Certificate Authority Set up for SSL would also be established as part of the Tender	CCA has SSL issuance guidelines in place which	The clause is sel explainanry and may accot=rdingly submite their bids.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
54	Bidders (ITB) -> 2.1 NIXI Pg. No. 16		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.	presently describes the issuance and hierarchy model. In the present guidelines SSL issuance is in offline mode and the CCA has a SPL root certificate (2022 / 2015) which is to be used for certifying the public keys of the CAs for issuing SSL & code signing certificates. Considering the above observation, please clarify the following points for us to provide an optimal solution: a. Going forward is NIXI going to manage the SSL Root CA (RCAI) on behalf of CCA. a.1. If yes, will there be a new Root Certificate created for this purpose or will the existing SPL Root CA be used? b. Please explain the hierarchy chain for SSL certificates to be issued c. Does the SSL DSC issuance follow the existing CCA's offline issuance guidelines or change in guidelines in accordance with WebTrust program is expected?	do-
55			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 RR Sites		do-
56	Section III: General Conditions of Contract (GCC) -> 6 Scope of work and Technical Specifications 5. THE OFFERED SOLUTION SHOULD INCLUDE THE FOLLOWING: Pg. No. 46	46	The proposed Root CA application software should provide all the modules from key life cycle management to CCA/CAs SSL certificates lifecycle management like creation, suspension, revocation etc. and should also cater the requirements as specified by CCA from time to time.		do-
57	Section III: General Conditions of Contract (GCC) -> 5.6 Confidentiality and IPR Rights -> 5.6.1 IPR Rights Pg. No. 42	42	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.	Software OEM provider offer COTS product for whose IPR rights solely rests with the OEM, hence we urge NIXI to modify the clause to any output / deliverable specially tailored for this deployment, the bidder / OEM needs to get approval of NIXI to reproduce.	do-
58	Section III: General Conditions of Contract (GCC) -> 6 Scope of work and Technical Specifications 5. THE OFFERED SOLUTION SHOULD INCLUDE THE FOLLOWING: Pg. No. 46	46	Suggesting 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.	As WebTrust certification is yet to be introduced for Indian CA environment, for wider participation of consultants we urge NIXI to relax this clause or modify the clause to remove the criteria of proven track record. It may be modified to "Suggesting 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"	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
59	Section IV: Bill of Material (BoM) -> Complete List of BoQ -> HARDWARE COMPONENTS Pg. No. 62	62	Hardware Security Module Network HSM - 3 Hardware Security Module USB HSM - 2	There is a difference of quantity in the number of HSMs given in both sections, please clarify.	The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
60	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> HARDWARE COMPONENTS Pg. No. 63	63	Hardware Security Module Network HSM - 5 Hardware Security Module USB HSM - 2		The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
61	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Software Components Pg. No. 63	63	Database - 2	Please clarify whether the number mentioned here refers to one license for each site. If so in DC two instances needs to be considered one for Production and another for Test setup. Hence we suggest NIXI to mention that these are indicative values while the Bidder may suggest the most optimal BOQ necessary for the deployment	The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
62	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Software Components Pg. No. 63	63	Servers - 8	Please clarify whether the numbers / quantity mentioned are only an indicative values or hard values. If these are hard values please explain the hardware and software deployment schematics in detail and also urge NIXI to provide a detailed diagram - * Contents to be installed in each server * Network diagram of DC (Production, Test) & DR sites	The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
63	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Professional Services Pg. No. 64	64	Operational Training On-site – 2 business Training months – Trainers	Please offer detailed note on the expectation / requirement for these training modules.	The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
64			Technical Training On-Site – Senior Technical Consultant (5 days)- Training based on location		

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
65	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support Pg. No. 66		Solution Software must support Windows Server 2016/2019, CentOS 8, Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 15.1, OpenSUSE Leap 15 operating systems	As the requirement is to support multi-platform we request to modify the clause to "Solution Software must support Windows Server 2016/2019 and Linux (any of the mentioned OS - CentOS 8, Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 15.1, OpenSUSE Leap 15) operating systems.	The bidder will ensure the exact no ofrequired HSM as per the WebTrust requireent and hence should include the items in BOQ and Price Bid format.
66	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support Pg. No. 66	66	Solution Software must support Microsoft SQL 2019, Oracle 19C, PostgreSQL 12, MySQL 8.0, MariaDB 10.x, SQLite 3.31 and Azure SQL databases.	As the requirement is to support popular database we request to modify the clause as follows. This offers the flexibility to Bidder to propose the database based on cost and expertise. "Solution Software must support one among the mentioned databases - Microsoft SQL 2019, Oracle 19C, PostgreSQL 12, MySQL 8.0, MariaDB 10.x, SQLite 3.31 and Azure SQL".	The bidder will ensure the database as pre WebTrust requirement.
67	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support -> point 7 Pg. No. 67	67	Cryptography support: RSA, RSASSA-PSS and ECDSA should be supported with SHA-2 of 256, 384 and 512. Hashing algorithms should be supported with key lengths as SHA-1,SHA- 224, SHA-256, SHA-384, and SHA-512. Support for end users keys with ECDSA and Edwards curves. CA certificates: CA signatures EdDSA: Ed25519 and Ed448	We request NIXI to limit the algorithms to existing CCA guideline and relax the requirement for Edwards Curves, ECDSA. We request to include support for RSA, ECC for public key algorithms only. As when the guidelines change, the Bidder should be able to comply with the changed guidelines related to algorithms.	No Change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
68	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support -> point 9 Pg. No. 67	67	The CA must support Secure key injection protocol (SKIP) that enables end to end protection of server generated key pairs for constrained devices/ servers	This RFP is for of issuing SSL certificates. Please explain the need for SKIP which are typically used for IOT devices. We request NIXI to remove the features that are not practically applicable to the purpose of this RFP.	The clause may be deleted. Bidder will ensure the requirements as per WebTrust.
69	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support -> point 10 Pg. No. 67	67	The CA must support butterfly cryptography to achieve high performance and low network load	Please explain the need for butterfly cryptography for issuance of SSL server certificates. Considering this RFP is only for SSL certificate issuance, performance and network load are not deterrent factors. If the feature is still required, we request detailed expectation on how and where it should be used. We request NIXI to remove the clauses/features not required for the purpose of this RFP to ensure that Bidder can optimise on the costs and offer only the relevant licenses.	The clause may be deleted. Bidder will ensure the requirements as per WebTrust.
70	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support -> point 11 Pg. No. 67	67	End entity key Management: It should be possible to encrypt, archive and recover end entity private keys (typically encryption keys) for the CA platform proposed and external CA's	This clause is relevant for issuance of Encryption keys rather than for SSL certificates. Hence requesting for removing this clause. We urge NIXI to remove the features that are not relevant for the purpose of this RFP to enable Bidder offer an optimal and cost effective solution	The clause may be deleted. Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
71	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Certificate Management interfaces -> point 1 Pg. No. 68	68	The solution must have powerful SOAP and REST based API supporting certification, revocation, suspension, resumption, renewal of certificate, certificate public key information fetching etc. with reasonable security controls based on TLS protocol and token authentication	Please clarify if the OEM can offer any industry standard token authentication model like JWT, if not please explain in detail the exact authentication model expected for APIs.	Bidder will ensure the requirements as per WebTrust.
72	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> CA Management -> point 6 Pg. No. 68	68	Ability to automate (via scripts) the creation of procedures, policies and profiles in the CA system	This requirement is an overkill for a SSL CA solution since the configuration / modification in a CA setup happens seldom. Unlike eSign setup where day-to-day addition of ASPs are required, frequent changes in policies here is not warranted. Further change in policies via scripts may not leave secure audit trail. Hence we request to relax this clause or modify the clause to "Provision to create procedures, policies and profiles in the CA system either automatically (via scripts) or via administration module"	Bidder will ensure the requirements as per WebTrust.
73	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> CA Management -> point 7 Pg. No. 68	68	Ability to populate values for the certificate's fields and extensions from parameters sent through web services.	Considering that NIXI has asked for an Registration Authority, typically all SSL issuance request would go via this module. So we request NIXI to modify the clause as suggested below: "*Ability to populate values for the certificate's fields and extensions from parameters sent through RA solution or web services.*"	Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
74	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Certificate Management interfaces -> point 5 Pg. No. 69	69	Must support not just EST– Enrolment over Secure Transport as per RFC 7030 and also EST over secure CoAP, IETF draft (draft ietf- ace-coap-est)	We request NIXI to remove the condition to support EST over secure CoAP as this feature is for issuance of certificates for iOT devices rather than SSL certificates for servers.	Bidder will ensure the requirements as per WebTrust.
75	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Certificate Management interfaces -> point 8 Pg. No. 69	69	Should support Windows Enrolment Proxy (WinEP) that facilitates enrolment to Microsoft Windows clients through native protocols.	Please explain the need for this clause for the purpose of issuance of SSL server certificates. We urge NIXI to remove the features that are not relevant for the purpose of this RFP to enable Bidder offer an optimal and cost effective solution.	Bidder will ensure the requirements as per WebTrust.
76	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Administrator Credential Management -> point 1 Pg. No. 69	69	The system must support storing keys and certificates on smart cards prepared with the card profiles in accordance with ISO/IEC 7816-15:2004, smart USB token, in PKCS#12 files and import them into the Windows certificate store of the end user device	In line with our existing CCA guidelines we urge NIXI to use PKI based authentication for CA solution using DSC in USB crypto token only.	Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
77	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Administrator Credential Management -> point 6 Pg. No. 69	69	During certification and smart card/ token issuing, it must be possible search and retrieve user data from one or more LDAP type of directories	This is required only for administrator users of the CA solution. The number is very low and the stated requirement would be an overkill. Hence we request to relax this clause.	Bidder will ensure the requirements as per WebTrust.
78	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Administrator Credential Management -> point 7 Pg. No. 69	69	Must support the administration of CA via both tightly integrated Java based thick client and centralized web-based GUI	Mandating thick client application will incur additional overheads for setup. We urge NIXI to modify the clause to use either Thick client or Web Based GUI	Bidder will ensure the requirements as per WebTrust.
79	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Scalability and Reliability -> point 2 Pg. No. 70	70	Should support Production rate of at-least 10,000 certificates requests per second.	Please clarify a. If the SSL certificate issuance is in offline mode as per CCA guidelines, the need for TPS does not arise. b. Even for Online issuance this number seems to be impractical, for number of reasons - * If the number of SSL certificates to be issued over 5 year period is 2 million, this translates to per day approx. 1600. * The certificate issuance needs to go through multiple approval process which requires manual intervention. Hence we request to arrive at optimal value, around 20 -	Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
80	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support Pg. No. 66	66	The solution must be properly scalable up to 2 million of users.	25 TPS. This will enable the Bidder to offer cost effective and optimal solution	Bidder will ensure the requirements as per WebTrust.
81	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 3 Pg. No. 70	70	Must support Common PKI (alias ISISMTT) v2.0 private extensions, private attributes and optional SigG-Profile.	We urge NIXI modify the clause to ensure the solution complies with CCA's existing guidelines for certificate profiles, attributes and extensions.	Bidder will ensure the requirements as per WebTrust.
82	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 5 Pg. No. 71	71	Must be compliant to issuing IEEE 1609.2 based certificates for CAs, sub Cas and end-entities	The IEEE standards mentioned here refers to "Wireless Access in Vehicular Environments (WAVE)", the feature mentioned here is primarily used in Cooperative Intelligent Transport Systems (C-ITS), an ecosystem to facilitate communication between vehicles and between vehicles and infrastructure. Considering this tender is for deploying SSL issuance we urge NIXI to remove this clause.	The clause may be deletd. Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
83	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 6 Pg. No. 71	71	Must support PKIX and ETSI Qualified Certificates	Request for relaxation of these clauses as they are specific to European telecommunication standards rather than Indian guidelines or WebTrust program.	Bidder will ensure the requirements as per WebTrust.
84	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 7 Pg. No. 71	71	Must support PSD2 Qualified Certificates, as specified in ETSI TS 119 495.		Bidder will ensure the requirements as per WebTrust.
85	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 8 Pg. No. 71	71	Must support OpenPGP V4 keys and certificates as per RFC 4880 and Extended Validation certificates		Bidder will ensure the requirements as per WebTrust.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
86	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 10 Pg. No. 71	71	Must support reverse proxy between CM clients (both SDK and thick clients) and the CM server. The SDK proxy can be used to prevent exposing the certificate issuance system being directly to external client.	The RFP requires a Registration Authority solution that prevents exposing CA solution to external clients. Please remove this clause.	The clause isself expalinary.
87	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 5 Pg. No. 72	72	The Timestamp server solution should support ESSCertIDv2, specified in ETSI 319 422	Request for relaxation of these clauses as they are specific to European telecommunication standards rather than Indian guidelines or webTrust program.	The clause isself expalinary.
88	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 6 Pg. No. 72	72	The Timestamp server should support NTP configuration to verify its local clock against UTC servers as specified in ETSI 319 421		The clause isself expalinary.
89	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 7 Pg. No. 72	72	The Timestamp server should support validating the private key usage period from the TS signing certificate as specified in ETSI 319 421		The clause isself expalinary.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
90	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 8 Pg. No. 72	72	The Timestamp server should provide filters that verifies user certificates for validation. The Filter should expect a user certificate to be sent through the chain. If no user certificate is provided, the filters should not continue and should throw an error. These filters should require SSL with client authentication enabled	Please explain the expected functionality and business use case for this clause in the context of issuance of SSL certificates. We urge NIXI to remove the features that are not relevant for the purpose of this RFP to enable Bidder offer an optimal and cost effective solution.	No change
91	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 1 Pg. No. 73	73	The system must support standard and creation of custom work flows unique to the organization for multiple levels of approvals 3 with BPMN 2.0 (Business Process Model and Notation).	Considering that the RFP is only for issuance of SSL certificates that follows a designated workflow for issuance, revocation, renewal, unlike an individual certificate issuance, the need for custom workflow model does not arise here. Hence we urge NIXI to relax this clause. We urge NIXI to remove the features that are not relevant for the purpose of this RFP to enable Bidder offer an optimal and cost effective solution.	No change
92	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 2 Pg. No. 73	73	The system must support storing keys and certificates on smartcards, smart USB token, in PKCS#12 files or import them into the 1 Windows certificate store of the end user device.	Please clarify the need for this clause. The key generation for SSL certificates are done by the clients and importing into their servers is also done by the clients. This clause appears to be specific to issuance of individual certificates. Further CCA guidelines do not permit for issuing certificates in soft format We urge NIXI to remove the features that are not relevant for the purpose of this RFP to enable Bidder offer an optimal and cost effective solution.	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
93	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 4 Pg. No. 73	73	The system must support end-user self-service functions for credential management tasks that can be performed by end users: PIN change, PIN unblocking, issuing, revocation, renewal, replacement as reasonable for different credential types (smart cards, PKCS#12 file, etc.)		No change
94	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 3 Pg. No. 73	73	The content of Crypto USB Tokens, smart cards and other credential forms should be configurable, e.g. number and purpose of certificates, key length, validity etc.	Considering that the RFP is only for issuance of SSL certificates the usage of Crypto token for certificate issuance is un-warranted as this clause is specific for individual DSC download.	No change
95	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 8 Pg. No. 73	73	The system must allow administrators to create templates for queries, reports, filters, and statistics.	The proposal solution offers custom filters for generating custom reports as per the needs of administrators. We urge NIXI to consider these options.	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
96	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 9 Pg. No. 73	73	The system must integrate with Active Directory and other corporate directories via LDAP v3 as data source and for batch synchronization to do scheduled import of user/device data from central repository like AD/ITSM system.	Unlike generic business application, a CA system will have very few admins with designated roles as described in the CCA guidelines. To manage these few admins this feature of syncing with external server is an overkill and sensitive. We recommend to remove this clause.	No change. Will be guided by WebTruist requitrements.
97	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 10 Pg. No. 73	73	The Solution should support contactless PKI cards together with the Mobile PKI app using NFC (near field communication). This will help address use cases where shared mobile devices are being used and individual users can use their contactless PKI card to identify and securely authenticate to the shared mobile device.	This feature is "out of scope" for SSL DSC issuance, this feature is useful for signing certificates. Hence we request not to include this clause.	No change. Will be guided by WebTruist requitrements.
98	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 11 Pg. No. 73	73	The system must support common smart card middleware, including Nexus Personal Desktop Client and other third-party vendors.	This clause refers to a proprietary OEM product's Client, which is contrary to spirit of Tender / RFP document. Hence this clause must be removed.	No change. Will be guided by WebTruist requitrements.

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
99	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 12 Pg. No. 73	73	The system must support integration with third party systems via JDBC, CSV and SCIM	As re-iterated earlier for identity management specially for CA solution, integration with 3rd party devices are not recommended considering the relatively very low number of admins to manage it. Hence we urge NIXI to offer explanation for this requirement or relax it.	No change. Will be guided by WebTruist requitrements.
100	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 13 Pg. No. 73	73	The system must be able to pre-register servers/devices details and should be able to blacklist/ whitelist entities for the automated issuance / management of device/server certificates	Please explain the requirement.	The clause is self explainanry.
101	Section V: Technical Specifications for the Equipment, Software and services -> Secure Access -> Pg. No. 74	74	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 to manage devices in CMS.	MFA is again overkill for CA solution, reasons being 1. The system will be accessed by administrators using PKI authentication where DSC is in USB token as per existing CCA guidelines. OTP and other methods are inferior	The clause is self explainanry.
			The solution should have a built-in Versatile Authentication Server (i.e. one server that provides different Authentication methods including PKI and OTP soft-tokens)	2 Multiple admins can be created each with designated roles and restricted access 3. Maker checker can be enabled to disable a single commit point	
			The solution should provide PKI soft tokens that can be installed on mobile phones such as iOS and Android.	For a CA solution usage of less vulnerable authentication factor like OTPs, or password tokens, biometric are not recommended. Even as per CCA guidelines PKI authentication is most recommended model. Moreover being an extremely sensitive system please explain the need to integrate external authentication services including RADIUS, SAML, Google authenticator for authenticating 5 - 6 admin roles in a CA solution. This entire feature list is an overkill. Request to relax these clauses since it requires to offer a full fledged MFA	The clause is self explainanry. No changes.
			The solution should provide soft tokens that generates One- Time-Passwords (OTP).		
			The solution should provide soft tokens that authenticate users based on a Challenge-Response algorithm.		do-
			The solution should provide Out-of-Band (OOB) Authentication via SMS and Email		do-

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
			The solution should provide OOB authentication with session binding.	solution and shoots the cost up.	do-
			The solution should provide OOB authentication using alpha- numeric OTPs. The length and the characters of the OTP should be configurable.		do-
			The Solution should support Google Authenticator and Microsoft Authenticator software tokens for generating One Time Passwords.		do-
			The PKI Software tokens should support the inbuilt Biometric capabilities of the mobile phones such as fingerprint ID and faceID.		do-
			The browser-based tokens should support all browsers like IE, Chrome, Firefox, Safari, and other mobile browsers.		do-
			The solution should be able to interoperate with other RADIUS servers		do-
			The solution should be compliant to the OATH reference architecture		do-
			The solution should support Identity Federation including both SAML v2 and Microsoft ADFS (Active Directory Federation Services)		do-
			The Solution should support OpenID Connect (OIDC).		do-
102	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 1 Pg. No. 74	74	To assist organizations to fulfill GDPR requirements, it should be possible to remove subject personal data from the CM database	Request for relaxation of these clauses as they are specific to European telecommunication standards rather than Indian guidelines or webTrust program.	No change
103	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 2 Pg. No. 74	74	Before removing user information, certificates that belongs to the user must be revoked	Request for relaxation of these clauses as they are specific to European telecommunication standards rather than Indian guidelines or webTrust program. We urge NIXI to ask the OEMs to abide by Indian CCA guidelines for revocation and record deletion process	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 3 Pg. No. 74	74	There should be control mechanisms on the server that ensures that revocation has been done before any subject data can be removed		No change
	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 4 Pg. No. 75	75	By use of SDK expired certificates and Audit Log records associated with the original certificate request should be removed from the database as well, for example after expiry of the certificate		The claus eis self explainanry
	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 5 Pg. No. 75	75	A new CM officer role should enable use of the subject removal functions.		The claus eis self explainanry
104	Section IV: Bill of Material (BoM)	61	Hardware Security Module (HSM)	HSM Certification Compliance : Since HSM's form the backbone of any security infrastructure, it is always backed up by corresponding security certifications. So, we would request NIXI to kindly to include certifications like FIPS 140-2 Level-3, CC, EAL 4+. Certification should be on the name of proposed OEM only; Certification on Third party OEM should not be considered. Please confirm the acceptance of our request.	No change
105	Section IV: Bill of Material (BoM)	61	Hardware Security Module (HSM)	Is doomsday service to be provided by existing OEM HSM Vendor for Key extraction (as plaintext key bytes) from existing HSM hardware ? We would request NIXI to kindly make it happen so that participation from different HSM OEMs is possible and does not restrict any OEM from participation.	No change

Sl. No.	Section No. / Clause No.	Page No.	RFP Content	Query / Suggestion	Response from NIXI
106	Section IV: Bill of Material (BoM)	61	Hardware Security Module (HSM)	(a) Please confirm if the current HSM have any multifactor authentication service / feature enabled. (b) Please provide the make, model and location wise (DC / DR) count of the existing HSM devices.	No change
107	Section IV: Bill of Material (BoM)	61	Hardware Security Module (HSM)	Does existing HSM OEM allow Keys to be migrated from its hardware to any other vendor's hardware device ? If not , then please clarify how can BCP be ensured in case vendor / OEM liquidates and goes out of existence?	No change
108	Section IV: Bill of Material (BoM)	61	Hardware Security Module (HSM)	Can the generation of new root key also be feasible while migrating to newer HSM ? Please clarify.	No change
109	Section IV: Bill of Material (BoM)	61, 62	Hardware Security Module (HSM)	There is a mention of requirement of Network HSM and USB HSM in the BoQ. We would request NIXI to clarify the desired TPS for Network HSM and USB HSMs keeping scalability as a key factor. Basis our understanding of the requirement we would recommend 4500 TPS(RSA-2048) to cater the current and near future requirements.	No change