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

Sr.No.	RFP Reference	Clause Description	Query	NIXI's Response
1	Section I: Notice Inviting Tender (NIT) -> 3.Eligibility Criteria for Participation in this Tender -> Point 2 Pg.No. 9	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.	To ensure wider participation we urge NIXI to relax the revenue requirement. We suggest to modify the clause to be changed to consider organizations whose balance sheets are profitable for last 3 years. Likewise similar to startup consider turnover relaxation for MSME organization too.	Not applicable as the work to be performed is one of the very specificalurity relating to PKI
2	Section II: Instructions to Bidders (ITB) -> 4.1.5 Support to Start-ups Pg.No. 20	Relaxation in Prior Turnover: Relaxation in the prior turnover for start-up enterprises (subject to meeting of quality & technical specifications) has been provided		
3	Section I: Notice Inviting Tender (NIT) -> 3.Eligibility Criteria for Participation in this Tender -> Point 2 Pg.No. 10	Not have a conflict of interest, which substantially affects fair competition.	Please explain / define what constitues conflict of interest for a bidder while submitting proposal	The existing CAS should not be a bidder doing the fornt ending
4	Section I: Notice Inviting Tender (NIT) -> 3.Eligibility Criteria for Participation in this Tender -> Point 4 Pg.No. 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
5	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 5 Pg.No. 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 empanneled auditor in the engagement.	No Change
6	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 1 Pg.No. 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
7	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 7 Pg.No. 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	The work is performed is very specific requirement. Hence no change
8	Section I: Notice Inviting Tender (NIT) -> Eligibility criteria for OEM (PKI Software): -> Point 8 Pg.No. 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.	Same as 07
9	Section II: Instructions to Bidders (ITB) -> 2.1 NIXI Pg.No. 16	Root Certificate Authority Set up for SSL would also be established as part of the Tender 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 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	CCA has SSL issuance guidelines in place which 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?	No Change
10	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	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.		SSL Root will be managed & maintained by CCA team only.
11	Section III: General Conditions of Contract (GCC) -> 5.6 Confidentiality and IPR Rights -> 5.6.1 IPR Rights Pg.No. 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.	As software OEM provider, we offer COTS product for whose IPR rights solely rests with the us, 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.	The IPR right for software/ Harware may be with some compant. However overall design of the system/ system architecture should be with CCA
12	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	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
13	Section IV: Bill of Material (BoM) -> Complete List of BoQ -> HARDWARE COMPONENTS Pg.No. 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 nos. mentioned in the final price bid format will be used for calculation of L1 & Nos ordered quality may very as per actual requirement
	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> HARDWARE COMPONENTS Pg.No. 63	Hardware Security Module Network HSM - 5 Hardware Security Module USB HSM - 2		
14	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Software Components Pg.No. 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	L1 will be calculated as per price bid formate.
15	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Software Components Pg.No. 63	Servers - 8	Please claify wherher 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	
16	Section IV: Bill of Material (BoM) -> Bill of Material for NIXI SSL Set Up -> Professional Services Pg.No. 64	Operational Training On-site – 2 business Training months – Trainers Technical Training On-Site – Senior Technical Consultant (5 days)- Training based on location	Please offer detailed note on the expectation / requirement for these training modules.	The bidder has to lead the team to Web Trust Certifier & training should be accordingly.

17	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	Bidder may go for his solution but it has to comply with web Trust criteria
18	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 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 clause may be accepted. However,the onus will be with the bidder to ensure WebTrust requirement.
19	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	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, as WebTrust Requirement need to be met.
20	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	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	No change, as WebTrust Requirement need to be met.
21	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	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 is self explanary.
22	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	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	No change, as WebTrust Requirement need to be met.
23	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	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.	No change, as WebTrust Requirement need to be met.
24	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	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 addtion 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 "Provsion to create procedures, policies and profiles in the CA system either automatically (via scripts) or via administration module"	The clause may be accepted. However,the onus will be with the bidder to ensure WebTrust requirement.
25	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	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 to "Ability to populate values for the certificate's fields and extensions from parameters sent through RA solution or web services."	No change, as WebTrust Requirement need to be met.
26	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	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.	No change, as WebTrust Requirement need to be met.
27	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	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	The clause is self explanary.
28	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	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 exisiting CCA guidelines we urge NIXI to use PKI based authentication for CA solution using DSC in USB crypto token only.	No change, as WebTrust Requirement need to be met.
29	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	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.	No change, as WebTrust Requirement need to be met.
30	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	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	No change, as WebTrust Requirement need to be met.
31	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	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	No change, as WebTrust Requirement need to be met.

32	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Platform support Pg.No. 66	The solution must be properly scalable up to 2 million of users.	The certificate issuance needs to go through multiple approval process which requires manual intervention. Hence we request to arrive at optimal value, around 20 - 25 TPS. This will enable the Bidder to offer cost effective and optimal solution	No change, as WebTrust Requirement need to be met.
33	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 3 Pg.No. 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 exisiting guidelines for certificate profiles, attributes and extensions.	No change, as WebTrust Requirement need to be met.
34	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 5 Pg.No. 71	Must be compliant to issuing IEEE 1609.2 based certificates for CAs, sub Cas and end-entities	The IEEE standards mentioned hee refers to "Wireless Access in Vehicular Environments (WAVE)", the feature metioned 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.	No change, as WebTrust Requirement need to be met.
35	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 6 Pg.No. 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	No change, as WebTrust Requirement need to be met.
36	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 7 Pg.No. 71	Must support PSD2 Qualified Certificates, as specified in ETSI TS 119 495.		No change, as WebTrust Requirement need to be met.
37	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 8 Pg.No. 71	Must support OpenPGP V4 keys and certificates as per RFC 4880 and Extended Validation certificates		No change, as WebTrust Requirement need to be met.
38	Section V: Technical Specifications for the Equipment, Software and services -> 1. Digital Certificate Lifecycle Management Solution (Minimum Specifications) -> Interoperability -> point 10 Pg.No. 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	No change, as WebTrust Requirement need to be met.
39	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 5 Pg.No. 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	No change, as WebTrust Requirement need to be met.
40	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 6 Pg.No. 72	The Timestamp server should support NTP configuration to verify its local clock against UTC servers as specified in ETSI 319 421		No change, as WebTrust Requirement need to be met.
41	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 7 Pg.No. 72	The Timestamp server should support validating the private key usage period from the TS signing certificate as specified in ETSI 319 421		No change, as WebTrust Requirement need to be met.
42	Section V: Technical Specifications for the Equipment, Software and services -> 3 Time Stamping Server -> point 8 Pg.No. 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	The claus eis self Explanary.
43	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 1 Pg.No. 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 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, as WebTrust Requirement need to be met.
44	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 2 Pg.No. 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	No change, as WebTrust Requirement need to be met.
45	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 4 Pg.No. 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.)	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, as WebTrust Requirement need to be met.
46	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 3 Pg.No. 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 certiicate issuance is un-warranted as this clause is specific for individual DSC download	No change, as WebTrust Requirement need to be met.
47	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 8 Pg.No. 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, as WebTrust Requirement need to be met.

48	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 9 Pg.No. 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 guidlines. To manage these few admins this feature of syncing with external server is an overkill and senstive. We recommend to remove this clause.	No change, as WebTrust Requirement need to be met.
49	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 10 Pg.No. 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, as WebTrust Requirement need to be met.
50	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 11 Pg.No. 73	The system must support common smart card middleware, including Nexus Personal Desktop Client and other third-party vendors.	This clause refers to a propreitary OEM product's Client, which is contrary to spirit of Tender / RFP document. Hence this clause must be removed	No change, as WebTrust Requirement need to be met.
51	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 12 Pg.No. 73	The system must support integration with third party systems via JDBC, CSV and SCIM	As re-iterated earlier for identity management specically 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.	The requirement should be as per WebTrust.
52	Section V: Technical Specifications for the Equipment, Software and services -> Workflow based lifecycle management module Specifications -> point 13 Pg.No. 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		No change, as WebTrust Requirement need to be met.
53	Section V: Technical Specifications for the Equipment, Software and services -> Secure Access -> Pg.No. 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 exisiting CCA guidelines. OTP and other methids are inferior 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 4. All logs and commit actions are digitally signed ensuring a fil-proof audit mechanisms. Considering we urge to relax these clauses 5. The specifications offered here requires offering a full fledged MFA solution which shoots the cost	No change, as WebTrust Requirement need to be met.
54		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)		No change, as WebTrust Requirement need to be met.
55		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 extermely senstive system please explain the need to integrate external authentiction 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 solution and shoots the cost up.	The requirement should be as per WebTrust.
56		The solution should provide soft tokens that generates One- Time-Passwords (OTP).		The requirement should be as per WebTrust.
57		The solution should provide soft tokens that authenticate users based on a Challenge-Response algorithm.		The requirement should be as per WebTrust.
58		The solution should provide Out-of-Band (OOB) Authentication via SMS and Email		The requirement should be as per WebTrust.
59		The solution should provide OOB authentication with session binding.		The requirement should be as per WebTrust.
60		The solution should provide OOB authentication using alpha- numeric OTPs. The length and the characters of the OTP should be configurable.		The requirement should be as per WebTrust.
61		The Solution should support Google Authenticator and Microsoft Authenticator software tokens for generating One Time Passwords.		The requirement should be as per WebTrust.
62		The PKI Software tokens should support the inbuilt Biometric capabilities of the mobile phones such as fingerprint ID and faceID.		The requirement should be as per WebTrust.
63		The browser-based tokens should support all browsers like IE, Chrome, Firefox, Safari, and other mobile browsers.		The requirement should be as per WebTrust.
64		The solution should be able to interoperate with other RADIUS servers		The requirement should be as per WebTrust.
65		The solution should be compliant to the OATH reference architecture		The requirement should be as per WebTrust.
66		The solution should support Identity Federation including both SAML v2 and Microsoft ADFS (Active Directory Federation Services)		The requirement should be as per WebTrust.
67		The Solution should support OpenID Connect (OIDC).		The requirement should be as per WebTrust.
68	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 1 Pg.No. 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	The requirement should be as per WebTrust.
69	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 2 Pg.No. 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	The requirement should be as per WebTrust.
70	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 3 Pg.No. 74	There should be control mechanisms on the server that ensures that revocation has been done before any subject data can be removed		The requirement should be as per WebTrust.
71	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 4 Pg.No. 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 requirement should be as per WebTrust.
72	Section V: Technical Specifications for the Equipment, Software and services -> 6 Data Privacy Functions -> point 5 Pg.No. 75	A new CM officer role should enable use of the subject removal functions.		The requirement should be as per WebTrust.
73	Generic	Generic	Request for extension of the Bid submission date by a week considering * The work needed to prepare and submit the bid * The forthcoming week being a festival season	Updated till 04 November, 2022