**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 Volume / Section | RFP Page No. | Content in the RFP | Clarification sought | NIXI's Respnse/Comments |
|---|---|---|---|---|---|
| 1 | Digital Certificate Lifecycle Management Solution (Minimum Specifications) | 66 | The CA must support Secure key injection protocol (SKIP) that enables end to end protection of server generated key pairs for constrained devices/ servers. | Not related to SSL. Request to remove the scope. | No Change, This requirement may come lateon. |
| 2 | IPR Rights | 43 | 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. | The IPR of the software is with the owner of the same. The IPR rights cannot be transferred. If needed, the source code can be escrowed based as per the arrangements made by NIXI and cost considerations. | Change as requested may be accepted, unless there is no WebTrust requirement and Bidder need to comply WebTrust Requiremens. |
| 3 | 5. THE OFFERED SOLUTION SHOULD INCLUDE THE FOLLOWING: | 45 | Fire Detection System- Smoke Detector,<br>VESDA,VESDA<br>Fire Suppression System- FM 200, CTV<br>Biometric Access Control (Dual Factor)<br>Water leakage Detector<br>Passive Infrared Sensor<br>Vibration Sensor<br>Rodent Repellents<br>Manned Security<br>Dual Precision AC<br>Dual UPS<br>Emergency Response Team<br>FRFC (2Nos)<br>Safe Locker (6 No | these Components doesn't appear in the BoQ. Please confirm that all these Components are part of BoQ and bidder has to consider or NIXI will provide at the time of implementation. | May be added as additional Line items, if the Bidder wishes. |
| 4 | Payment Terms | 55 | Complete Delivery, Commissioning andacceptance per site<br><br>70 % value of contract price Installation, pertaining to equipment(s) at individual site | The scope of project has significant hardware delivery. Request to reconsider the payment terms of the hardware by making full payment on delivery of the items. Software/Services payment can be connected with project milestones. | No, changes |
| 5 | Infrastructure Items | 45 | Items related to physical infrastucture | There are items mentioned in the scope related to physical infrastructure including fire detection systems, AC etc. The same is not available in the BOM. As the complete specifications can be accessed only after the physical inpection of the site, request to remove from the scope. NIXI datacenter may have these equipments already. | In the Initail stage, there no reqirements for the AC works. However, Fire detection syatems needs to be part of the Smart Rack. Bidder may incorporate the cost accordingly. |
| 6 | Digital Certificate Lifecycle Management Solution (Minimum Specifications) | 66 | The CA must support butterfly cryptography to achieve high performance and low network load | Related to blockchain and crypto currency. Request to remove the scope. | The bidder will ensure the WebTrust Requirement. Otherwise, the clause may be relaxed. |
| 7 | CA Management | 68 | Ability to automate (via scripts) the creation of procedures, policies and profiles in the CA system | Complied: Is it expected to automate creation of procedures and policies. This may lead to unwarranted vulnerabilities in the system. Request to ignore the scope. | No Change, This requirement may come lateon. |
| 8 | Certificate Management interfaces | 69 | Should support Windows Enrolment Proxy (WinEP) that facilitates enrolment to Microsoft Windows clients through native protocols. | This is not relevant for SSL. Request to ignore the scope. | No change, as there may be future requirement for other scopes in NIXI. |
| 9 | Administrator Credential Management | 69 | The system must support delegated certificate issuing, revocation, renewal, temporary replacement, permanent replacement, PIN unblocking with PUK, PIN reset, and PIN change should be possible at remote clients in a secure way | Whole section is not relevant for SSL. Request to ignore the scope. | No change, as there may be future requirement for other scopes in NIXI. |
| 10 | Administrator Credential Management | 69 | The content of smart cards / tokens and other credential forms should be configurable, e.g. number and purpose of certificates, key length, validity etc. | Whole section is not relevant for SSL. Request to remove the scope. | No change, as there may be future requirement for other scopes in NIXI. |
| 11 | Administrator Credential Management | 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 | Whole section is not relevant for SSL . Request to remove the scope. | No change, as there may be future requirement for other scopes in NIXI. |
| 12 | Time Stamping Server | 72 | The Timestamp server solution should support ESSCertIDv2, specified in ETSI 319 422 | If the operations are performed in India then why ETSI is required. Also the whole criteria is webtrust | No change, as there may be future requirement for other scopes in NIXI. |
| 13 | Workflow based lifecycle management module Specifications | 73 | The system must support storing keys and certificates on smart cards, smart USB token, in PKCS#12 files or import them into the Windows certificate store of the end user device. | For SSL certificates smart card and USB does not make sense | No change, as there may be future requirement for other scopes in NIXI. |
| 14 | Workflow based lifecycle management module Specifications | 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. | Need more clarity. May not be relevant for SSL. | The clause is self explanary and prospective bidders may accordingly respond |
| 15 | Secure Access | 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. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 16 | Secure Access | 74 | 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) | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 17 | Secure Access | 74 | The solution should provide PKI soft tokens that can be installed on mobile phones such as iOS and Android. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 18 | Secure Access | 74 | The solution should provide soft tokens that generates One-Time-Passwords (OTP). | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |

| | | | | | |
|---|---|---|---|---|---|
| 19 | Secure Access | 74 | The solution should provide soft tokens that authenticate users based on a Challenge-Response algorithm. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 20 | Secure Access | 74 | The solution should provide Out-of-Band (OOB) Authentication via SMS and Email | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | No Change |
| 21 | Secure Access | 74 | The solution should provide OOB authentication with session binding. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | No Change |
| 22 | Secure Access | 74 | The solution should provide OOB authentication using alphanumeric OTPs. The length and the characters of the OTP should be configurable. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | No Change |
| 23 | Secure Access | 74 | The Solution should support Google Authenticator and Microsoft Authenticator software tokens for generating One Time Passwords. | Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 24 | Secure Access | 74 | The PKI Software tokens should support the inbuilt Biometric capabilities of the mobile phones such as fingerprint ID and faceID. | Maynot be relevant for the context of SSL. . Request to remove the scope. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 25 | Data Privacy Functions | 74 | Data Privacy Functions | This section can be changed to "Compliance to Indian Data Privacy regulation" | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 26 | Data Privacy Functions | 74 | To assist organizations to fulfill GDPR requirements, it should be possible to remove subject personal data from the CM database. | This is not relevant for Indian context. | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 27 | Data Privacy Functions | 74 | Before removing user information, certificates that belongs to the user must be revoked | This appears to be wrt individual certificate related not for SSL certificates | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 28 | Data Privacy Functions | 74 | There should be control mechanisms on the server that ensures that revocation has been done before any subject data can be removed | This appears to be wrt individual certificate related not for SSL certificates | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 29 | Data Privacy Functions | 74 | 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 | This appears to be wrt individual certificate related not for SSL certificates | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 30 | Data Privacy Functions | 74 | A new CM officer role should enable use of the subject removal functions. | This appears to be wrt individual certificate related not for SSL certificates | May be accpted. However, the bidder will ensure WebTrust requirement. |
| 31 | Bill of Material for NIXI SSL Set Up, Hardware Components | 62 | HARDWARE COMPONENTS | Our understanding is that the Hardware and software details are provided in the RFP which includes both DC & DR environments. Kindly confirm the same. Also, the QA environment is not considered, shall we consider the same as part of BOQ, kindly confirm. | May include as line itme in Price bid, if the bidder finds it essential for WebTrust. |
| 32 | g. Scalability and Reliability | 70 | Should support Production rate of at-least 10,000 certificates requests per second. | Kindly confirm the stated requirement as it my not be relevant for the SSL context. | May include as line itme in Price bid, if the bidder finds it essential for WebTrust. |
| 34 | SWAPPABLE COMPONENTS | 93 | Migration Model | Our understanding is that migration is not required as this is the new CA setup. Please confim, what is the expected migration activity to be carried out for this project? | The clause is self expananry and bidder may use due diligence on the matter in the perspective of WebTrust. |