Expression of Interest (EOI) – Registry Services Platform

***[Disclaimer:** This Registry Services Platform is being designed and developed for upcoming new generic top-level domains (New gTLDs)]*

Request for Technical Proposal – Creating India's Registry Platform

Expression of Interest (EoI)

For Registry Services Platform (RSP) for new gTLDs Domain and IDNs

Issued by:
National Internet Exchange of India (NIXI)
B-901 9th Floor,
Tower B, World Trade Center,
Nauroji Nagar,
New Delhi 110029, India

EOI Reference: NIXI/Tech/006/02-2025
Date: 01-08-2025

Background:

The .IN Country Code Top-Level Domain (ccTLD) and 22 Indian-language Internationalized Domain Names (IDNs) are managed by NIXI as a trusted custodian of India's digital identity. In line with the *Digital India* vision and the Government of India's push for technological sovereignty, NIXI, invites Expressions of Interest (EoI) from reputed software providers and system integrators to build, deploy, and maintain a world-class, scalable, and secure in-house Registry Services Platform (RSP), to be used for upcoming new gTLD.

This initiative will place India at the forefront of next-generation internet infrastructure and promote self-reliance in critical digital systems.

Scope of the RSP Solution:

The proposed RSP platform must support:

- Shared Registry System (SRS) with EPP, DNSSEC, RDAP, WHOIS, IPv6 support.
- Registry-Registrar integrations, multilingual domain support (IDNs).
- Centralized billing, wallet system, and lifecycle management (auto-renewals, deletions).
- Real-time abuse detection, compliance, and reporting systems.
- Modular, cloud-native, scalable architecture ensuring high availability, resilience, security and ICANN-compliant operations.
- Real time transition from present Technical Services Provider (TSP) including (but not limited to) registrar billing and customer support
- The platform will be delivered on a Build, Operate Transfer (BOT) model with all source code and rights. All IP will be the property of NIXI post transfer.

Who Can Apply:

EOIs are invited from:

- Indian or global technology firms with prior experience in registry, fintech, telecom, or critical infrastructure systems AND a presence in India.
- Firms with demonstrated expertise in building scalable, secure, and standards-compliant internet systems.
- ICANN-accredited or RSP-evaluation-ready entities will be preferred.
- The Bidder should be registered as Indian company registered under Companies Act, 1956 (2013) or as amended or a LLP firm/ Partnership firm under Partnership Act 1932.
- The bidder must be in existence for at least 7 years with minimum annual average turnover of INR 50 crores each and positive net-worth for the last three financial years (FY 2022-23, 2023-24 and 2024- 25) with at least 5 years of operations in India as on bid submission date.
- The bidder can also be in the form of a consortium /JV/SPV as long as turnover requirements as outlined above are met. Net worth requirements for purposes of qualification will be of the primary/lead bidding organization.

Submission Guidelines:

Interested parties must submit the following:

- Company profile and relevant project experience.
- Technical proposal outline (architecture, timeline, and compliance).
- Delivery model (in-house, co-development, or consortium).
- High-level commercials and engagement model.

Please email your EOI to:
Submission Deadline: 29.08.2025

NIXI plans to have a stakeholder meeting on 14.08.2025 to discuss any queries that the bidder/s might have. Post the meeting with stakeholders, NIXI will issue a comprehensive RFP for bidders.

Please note that only those parties/bidders that have emailed NIXI prior to 13.08.2025 will be allowed to participate in the meeting on 14.08.2025.

Why Partner with NIXI:

NIXI is at the heart of India's digital infrastructure, working closely with MeitY and international internet governance bodies like ICANN and IANA. As a progressive, technology-forward organization, NIXI is building an open, secure, multilingual internet ecosystem. Be part of shaping India's digital future.

Annexure

Suggested Registry Platform Architecture & Components.

The Registry platform, architecture, components, functionality and features are suggestive in nature and outline NIXI's overall requirement. These may be changed, modified, deleted by NIXI based on inputs from stakeholders and/or in consideration of global best practices.

Registration Services: Core Functionality and Advanced Features

The proposed registry platform should be designed to provide comprehensive, robust, and efficient registration services, ensuring seamless domain name management for new gTLDs namespaces. We understand the critical importance of a reliable and high-performance registration system for both registrars and end-users. The solution should incorporate the following key features:

1. Real-Time Domain Name Registration, Renewal, and Transfer Functionalities:

A. Real-Time Processing:
   a. The platform will facilitate real-time processing of all registration, renewal, and transfer requests. This ensures immediate updates to the registry database and DNS, minimizing delays and enhancing user experience.
   b. The platform will utilize optimized database queries and caching mechanisms to achieve sub-second response times, even during peak traffic periods.

B. Automated Validation:
   a. The platform will incorporate robust automated validation checks to ensure data accuracy and compliance with registry policies.
   b. This will include validation of domain name syntax, length, character sets, and compliance with IDN registration rules.

C. Transaction Logging and Auditing:
   a. All registration, renewal, and transfer transactions will be meticulously logged and audited, to ensure transparency, accountability, and facilitate dispute resolution.

D. Bulk Operations:
   a. The platform will support bulk operations for registrars, enabling them to efficiently manage large volumes of domain names.
   b. This includes bulk registration, renewal, transfer, and modification of domain name data.

E. Domain Name Availability Checks:

a. The platform will provide fast and accurate domain name availability checks through a user-friendly API and web interface, to enable registrars and end-users to quickly determine the availability of desired domain names.

2. Support for Various Registration Periods and Pricing Models:

A. Flexible Registration Periods:

a. The platform should support a wide range of registration periods, from one year to multiple years, as determined by NIXI's policies that will provide registrars with the flexibility to offer diverse registration options to their customers.

B. Tiered Pricing Models:

a. The system will be designed to accommodate various pricing models, including tiered pricing, promotional pricing, and volume discounts.

C. Automated Price Calculation:

a. The platform should automatically calculate registration, renewal, and transfer fees based on the selected registration period and pricing model.

D. Currency Support:

a. The system should support the Indian Rupee, for transaction purposes and should have the flexibility to support other international currencies as required by NIXI.

E. Promotional Capabilities:

a. The platform should have the ability to run temporary promotions, and coupon codes for various tenures and domain actions.

3. Implementation of EPP (Extensible Provisioning Protocol) for Seamless Communication with Registrars:

A. EPP Compliance:

a. The platform will fully comply with the EPP standard, ensuring seamless communication with registrars to enable registrars to efficiently manage domain names using industry-standard protocols.

B. EPP Extensions:

a. Relevant EPP extensions must be implemented to support specific requirements of the new gTLDs namespaces.

C. Secure EPP Communication:

a. All EPP communication should be secured using TLS/SSL encryption to protect sensitive data.

D. EPP Testing and Certification:

a. Comprehensive EPP testing and certification tools must be incorporated to ensure compatibility with registrars' systems.

E. EPP Command Support:

a. EPP implementation should support all necessary EPP commands, including domain:check, domain:create, domain:renew, domain:transfer, domain:info, domain:update, and domain:delete.

Additional Considerations:

1. **API Availability:**
   In addition to EPP, APIs should be available for registrars to integrate with the platform
2. **Scalability and Performance:**
   The platform should be designed to handle high volumes of registration requests and ensure optimal performance, benchmarked against global standards.
3. **Security:**
   Security by design philosophy should be followed to ensure that the registry data is secured, global security best practices are followed.
4. **Reporting:**
   Detailed reports/ dashboards on registration activity, trends, and statistics should be part of the platform

DNS Management: Ensuring High-Performance, Secure, and Reliable Domain Name Resolution

The platform should incorporate a robust and highly efficient DNS (Domain Name System) management system, designed to guarantee reliable domain name resolution.

1. High-Performance, Distributed DNS Infrastructure for Reliable Domain Name Resolution:

A. **Distributed Architecture:**
   DNS infrastructure should be designed with a distributed architecture, utilizing multiple geographically dispersed name servers.

B. **Anycast Networking:**
   Anycast networking to route DNS queries to the nearest available name server should be implemented.

C. **Caching Mechanisms:**
   DNS servers should employ advanced caching mechanisms to store frequently accessed DNS records and reducing load on the registry database and improving query response times.

D. **High Availability:**
DNS infrastructure should be engineered for high availability, with redundancy built in for hardware and software) with no single point of failure.

E. **Load Balancing:**
Load balancing techniques/best practices, to distribute DNS queries evenly across name servers, should be implemented.

F. **Monitoring and Alerting:**
A comprehensive monitoring and alerting systems to track the performance and health of DNS infrastructure must be implemented.

2. Support for DNSSEC (Domain Name System Security Extensions) to Enhance Security:

A. **DNSSEC Implementation:**
The platform will fully support DNSSEC, enabling domain owners to digitally sign their DNS records.

B. **Key Management:**
Secure key management tools for generating, storing, and managing DNSSEC keys must be provided.

C. **Automated Signing:**
The platform should support automated signing of DNS records, reducing the manual effort required to maintain DNSSEC.

D. **Validation and Monitoring:**
Tools for validating and monitoring DNSSEC signatures, ensuring the integrity of DNS data, must be provided.

E. **DNSSEC Compliance:**
DNSSEC implementation will comply with all relevant industry standards and best practices.

3. Tools for Managing DNS Records (A, AAAA, CNAME, MX, etc.):

A. **User-Friendly Interface:**
A user-friendly interface for registrars and domain owners to manage DNS records must be provided

B. **API Access:**
A robust API for programmatic access to DNS record management must be provided.

C. **Record Type Support:**

a. The platform will support all standard DNS record types, including:
   1. A (Address) records
   2. AAAA (IPv6 Address) records
   3. CNAME (Canonical Name) records
   4. MX (Mail Exchange) records

5. TXT (Text) records
6. NS (Name Server) records
7. SRV (Service) records
8. And more.

D. **Record Validation:**
The platform should validate DNS records to ensure they comply with DNS standards.

E. **Zone Management:**
Tools for managing DNS zones, including creating, modifying, and deleting zones should be provided.

F. **Dynamic DNS Support:**
Dynamic DNS should be supported by the platform.

Additional Considerations:

A. **IPv6 Support:**
DNS infrastructure will fully support IPv6, ensuring compatibility with the latest internet protocols.

B. **Performance Optimization:**
Platform should continuously optimize DNS infrastructure for performance, ensuring fast and reliable domain name resolution.

C. **Security Audits:**
regular security audits of DNS infrastructure to identify and address potential vulnerabilities should be conducted.

D. **Compliance:**
Platform DNS management system should comply with all relevant industry standards and regulations.

WHOIS/RDAP Services: Providing Accurate and Compliant Domain Name Information Lookup

Proposed registry platform will implement comprehensive WHOIS and RDAP (Registration Data Access Protocol) services, ensuring accurate and accessible domain name information lookup. Understanding the importance of balancing transparency with data privacy, the platform will adhere to all relevant regulations and best practices.

1. Implementation of Robust WHOIS and RDAP Services for Domain Name Information Lookup:

A. **WHOIS Service:**

   a. The platform will provide a robust and reliable WHOIS service, allowing users to query domain name registration information.

   b. The WHOIS service will be designed for high performance and scalability, ensuring fast and accurate responses.

   c. Appropriate rate limiting and security measures to prevent abuse and protect the service, will be implemented on the platform.

   d. The WHOIS service will be available through both web-based and command-line interfaces.

B. **RDAP Service:**

   a. A fully compliant RDAP service, adhering to the latest IETF standards, will be implemented.

   b. RDAP implementation will support all relevant RDAP extensions and features.
   and will support JSON responses.

C. **Data Accuracy and Consistency:**

   a. data validation and verification procedures should be implemented to ensure the accuracy and consistency of domain name registration information and the platform should automatically synchronize data between the registry database and the WHOIS/RDAP services.

D. **Search and Filtering:**

   a. WHOIS/RDAP service will provide advanced search and filtering capabilities, allowing users to easily find specific domain name information including search by domain name, registrar, registrant, and other relevant criteria.

E. **API Access:**

   a. A robust API for programmatic access to the WHOIS/RDAP services, enabling registrars and developers to integrate domain name information lookup into their applications should be provided.

2. Compliance with Data Privacy Regulations:

- **Data Minimization:**
  - Adherence to the principle of data minimization, collecting only the necessary information for domain name registration must be incorporated at design level
- **Data Protection:**
  - We robust security measures to protect domain name registration data from unauthorized access, use, or disclosure must be implemented
  - Measures could include encryption, access controls, and regular security audits.
- **Data Retention:**

  - establish clear data retention policies, specifying the duration for which domain name registration data will be stored.
  - data retention policies will comply with all applicable legal and regulatory requirements.
- **Data Access and Correction:**
  - provide mechanisms for domain owners to access and correct their domain name registration data.
- **Redaction and Anonymization:**
  - implement appropriate redaction and anonymization techniques to protect sensitive personal information in the WHOIS/RDAP responses.
  - This will be done in accordance with relevant laws of India.
- **Compliance with Indian Data Privacy Laws:**
  - ensure full compliance with all applicable data privacy laws in India, including the Information Technology Act, 2000, and any relevant subsequent legislation.
- **Transparency:**
  - provide clear and transparent information about our data collection, use, and disclosure practices.
  - provide clear information on the user's rights.

Additional Considerations:

A. **Performance Optimization:**
   a. continuously optimize our WHOIS/RDAP services for performance, ensuring fast and efficient responses.

B. **Security Audits:**
   a. conduct regular security audits of our WHOIS/RDAP services to identify and address potential vulnerabilities.

C. **International Standards:**
   a. WHOIS/RDAP implementation will comply with relevant international standards and best practices.

Registry Data Management: Ensuring Secure, Scalable, and Reliable Storage and Analysis of Domain Name Registration Data proposed registry platform will feature a robust and comprehensive registry data management system, designed to securely store, manage, and analyze domain name registration data for new gTLDs namespaces.

1. Secure and Scalable Database for Storing Domain Name Registration Data:

A. **Database Selection:**

a. utilize a high-performance, scalable, and secure database system, such as PostgreSQL, MySQL, or a distributed NoSQL database, depending on NIXI's specific requirements.

b. The chosen database will be capable of handling large volumes of data and high transaction rates.

B. **Data Encryption:**

a. All domain name registration data will be encrypted at rest and in transit, using industry-standard encryption algorithms.

C. **Access Control:**

a. implement granular access control mechanisms to restrict access to registry data based on user roles and permissions.

D. **Data Integrity:**

a. implement data integrity checks to ensure the accuracy and consistency of domain name registration data.

b. This will include data validation rules, checksums, and other integrity checks.

E. **Scalability:**

a. database architecture will be designed for horizontal and vertical scalability, allowing it to handle future growth in data volume and transaction rates.

F. **Performance Optimization:**

a. optimize database queries and indexes to ensure fast and efficient data retrieval.

2. Data Backup and Recovery Mechanisms:

A. **Automated Backups:**

a. implement automated backup procedures to regularly back up the registry database.

b. Backups will be stored in geographically diverse locations to ensure data redundancy.

B. **Incremental Backups:**

a. utilize incremental backups to minimize backup times and storage requirements.

C. **Point-in-Time Recovery:**

a. system will support point-in-time recovery, allowing us to restore the database to a specific point in time in the event of data loss.

D. **Disaster Recovery Plan:**

a. develop a comprehensive disaster recovery plan to ensure business continuity in the event of a major disruption.

b. This will include procedures for data recovery, system restoration, and communication.

E. **Regular Testing:**

a. conduct regular testing of our backup and recovery procedures to ensure their effectiveness.

3. Reporting and Analytics Tools:

A. **Customizable Reports:**
   a. provide customizable reporting tools that allow NIXI to generate reports on various aspects of domain name registration data.
   b. This will include reports on registration trends, registrar activity, and other relevant metrics.

B. **Real-Time Dashboards:**
   a. implement real-time dashboards that provide NIXI with an overview of key registry metrics.

C. **Data Visualization:**
   a. Utilize data visualization techniques to present registry data in a clear and concise manner.

D. **Data Export:**
   a. Provide tools for exporting registry data in various formats (e.g., CSV, JSON).

E. **API Access:**
   a. Provide API access to registry data, enabling NIXI to integrate the data with other systems.

F. **Analytics Capabilities:**
   a. Provide tools that can help analyze trends, and provide predictive analytics.

Additional Considerations:

A. **Data Retention Policies:**
   a. implement data retention policies that comply with all applicable legal and regulatory requirements.

B. **Data Security Audits:**
   a. conduct regular security audits of our registry data management system to identify and address potential vulnerabilities.

C. **Performance Monitoring:**
   a. continuously monitor the performance of our registry data management system to ensure optimal efficiency.

D. **Compliance:**
   a. The registry data management system will comply with all relevant industry standards and regulations.

Billing and Accounting: Streamlining Financial Operations for Registrars and NIXI

proposed registry platform will incorporate a comprehensive and automated billing and accounting system, designed to streamline financial operations for both registrars and NIXI.

1. Automated Billing and Invoicing System for Registrars:

a. **Automated Invoice Generation:**
System will automatically generate invoices for registrars based on their domain name registration, renewal, and transfer activities.

b. **Flexible Billing Cycles:**
Support flexible billing cycles, allowing NIXI to define billing periods based on their operational requirements. This could include monthly, quarterly, or annual billing cycles.

c. **Customizable Invoice Templates:**
System will allow NIXI to customize invoice templates to reflect their branding and specific requirements.

d. **Automated Payment Reminders:**
System will automatically send payment reminders to registrars, reducing the need for manual follow-up.

e. **Credit Management:**
Platform will provide credit management features, allowing NIXI to set credit limits for registrars.

f. **Dispute Management:**
System will facilitate dispute management, allowing registrars to raise and resolve billing disputes efficiently.

g. **API Integration:**
Provide a robust API for registrars to integrate our billing system with their own accounting and CRM systems.

2. Support for Various Payment Methods:

A. **Online Payment Gateways:**
   a. integrate with popular online payment gateways to support various payment methods, including credit cards, debit cards, net banking, and UPI.
   b. This will provide registrars with flexible payment options.

B. **Bank Transfers:**
   a. system will support bank transfers, allowing registrars to make payments directly from their bank accounts.

C. **Prepaid Accounts:**
   a. support prepaid accounts, allowing registrars to deposit funds in advance and use them for domain name registration and other services.

D. **Payment Reconciliation:**
   a. system will automatically reconcile payments with invoices, ensuring accurate accounting records.

3. Financial Reporting and Reconciliation Tools:

A. **Detailed Financial Reports:**
   a. provide detailed financial reports, including revenue reports, transaction reports, and payment reports.

B. **Customizable Reports:**
   a. system will allow NIXI to customize financial reports based on their specific requirements.

C. **Real-Time Dashboards:**
   a. implement real-time dashboards that provide NIXI with an overview of key financial metrics.

D. **Automated Reconciliation:**
   a. system will automate the reconciliation of financial transactions, ensuring accurate accounting records.

E. **Audit Trails:**
   a. system will maintain detailed audit trails of all financial transactions, ensuring transparency and accountability.

F. **Data Export:**
   a. provide tools for exporting financial data in various formats (e.g., CSV, Excel).

Additional Considerations:

A. **Currency Support:**
   a. system will support the Indian Rupee, and if needed, other currencies.

B. **Tax Compliance:**
   a. system will comply with all relevant tax regulations in India.

C. **Security:**
   a. implement robust security measures to protect financial data from unauthorized access.

D. **Integration:**
   a. system will be designed to integrate with NIXI's existing accounting and financial systems.

Security Infrastructure: Implementing Robust Measures to Safeguard Registry Data and Systems

proposed registry platform will be built with a robust and layered security infrastructure, designed to protect registry data and systems from a wide range of threats.

1. Implementation of Robust Security Measures to Protect Registry Data and Systems:

A. **Data Encryption:**

a. All sensitive data, including domain name registration information, financial data, and user credentials, will be encrypted at rest and in transit using industry-standard encryption algorithms (e.g., AES-256, TLS 1.3).
b. Encryption keys will be securely managed and rotated regularly.

B. **Access Control:**
   a. implement granular role-based access control (RBAC) to restrict access to registry data and systems based on user roles and permissions.

C. **Authentication and Authorization:**
   a. enforce strong authentication and authorization mechanisms, including multi-factor authentication (MFA), to protect against unauthorized access.
   b. implement secure password policies and regularly audit user accounts.

D. **Firewall and Network Security:**
   a. deploy robust firewalls and network security devices to protect the registry network from unauthorized access and malicious traffic.
   b. implement network segmentation to isolate critical systems.

E. **Web Application Security:**
   a. implement secure coding practices and web application firewalls (WAFs) to protect against web-based attacks, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

F. **Operating System and Application Hardening:**
   a. harden operating systems and applications to minimize vulnerabilities and reduce the attack surface.
   b. This may include disabling unnecessary services, applying security patches, and configuring secure system settings.
   c.

G. **Secure Software Development Lifecycle (SSDLC):**
   a. follow a secure software development lifecycle (SSDLC) to ensure that security is integrated into every stage of the development process.
   b. include security requirements analysis, threat modeling, secure coding practices, and security testing.

H. **Regular Security Patching:**
   a. implement a robust patch management system to ensure that all systems are regularly updated with the latest security patches.

2. Intrusion Detection and Prevention Systems (IDPS):

A. **Network-Based IDPS:**
   a. deploy network-based intrusion detection and prevention systems (IDPS) to monitor network traffic for malicious activity.

B. **Host-Based IDPS:**

   a. deploy host-based IDPS to monitor system logs and file integrity for signs of intrusion.

C. **Security Information and Event Management (SIEM):**
   a. implement a security information and event management (SIEM) system to collect and analyze security logs from various sources.

D. **Real-Time Monitoring and Alerting:**
   a. implement real-time monitoring and alerting systems to notify security personnel of suspicious activity.

E. **Incident Response Plan:**
   a. develop a comprehensive incident response plan to guide our response to security incidents.
   b. This may include procedures for incident detection, containment, eradication, and recovery.

3. Regular Security Audits and Vulnerability Assessments:

A. **Regular Vulnerability Scans:**
   a. conduct regular vulnerability scans of our systems to identify potential weaknesses.
   b. This may include scans for known vulnerabilities in operating systems, applications, and network devices.

B. **Penetration Testing:**
   a. engage independent security experts to conduct regular penetration testing of systems.

C. **Security Audits:**
   a. conduct regular security audits of our systems and processes to ensure compliance with industry standards and best practices.
   b. This may include audits of access controls, data security, and incident response procedures.

D. **Security Awareness Training:**
   a. provide regular security awareness training to all personnel to ensure that they understand their role in protecting registry data and systems.
   b. include training on phishing awareness, password security, and other security best practices.

E. **Compliance:**
   a. comply with all relevant industry standards and regulations, including ISO 27001, PCI DSS (if applicable), and any relevant Indian government regulations.

Scalability and Performance: Ensuring High Availability and Responsiveness for new gTLDs Registry Services

proposed registry platform must be designed with a focus on scalability and performance, ensuring that it can handle current and future demands.

1. Handling High Volumes of Registrations and DNS Queries:

A. **Optimized Database Architecture:**
   a. employ a database architecture optimized for high-volume transactions and queries. This will include indexing strategies, query optimization, and efficient data partitioning.
   b. utilize database caching mechanisms to reduce the load on the database and improve response times.

B. **Load Balancing and Distribution:**
   a. platform will incorporate load balancing techniques to distribute traffic evenly across our servers, ensuring optimal performance during peak periods.
   b. utilize a distributed architecture for our DNS infrastructure, enabling it to handle a large volume of DNS queries efficiently.

C. **Asynchronous Processing:**
   a. implement asynchronous processing for non-critical tasks, such as background data processing and reporting, to minimize the impact on real-time operations.

D. **Caching Mechanisms:**
   a. implement caching mechanisms at multiple levels, including application-level caching, database caching, and DNS caching, to reduce response times and improve overall performance.

E. **Efficient Code and Algorithms:**
   a. software will be developed using efficient coding practices and algorithms to minimize resource consumption and improve performance.
   b. conduct thorough performance testing and optimization throughout the development process.

2. Platform Architecture for Horizontal and Vertical Scaling:

- **Horizontal Scaling:**
  - The platform should be designed for horizontal scaling, allowing addition of servers to increase capacity as needed.

1. Platform's Redundancy and Failover Mechanisms:

A. **Redundant Hardware and Infrastructure:**

   a. redundant hardware and infrastructure components, including servers, network devices, and storage systems to be incorporated to reduce/eliminate single point of failure.

B. **Failover Mechanisms:**

   a. implement automatic failover mechanisms to switch to redundant systems in the event of a hardware or software failure.

C. **Load Balancing and Distribution:**

   a. load balancing to distribute traffic across multiple servers should be deployed.

D. **Database Replication and Clustering:**

   a. implement database replication and clustering to ensure data redundancy and high availability.

E. **DNS Redundancy:**

   a. DNS infrastructure and architecture should be designed with multiple geographically dispersed name servers, ensuring redundancy and high availability.

2. Disaster Recovery Plan:

- **Data Backup and Recovery:**
  - implement a robust data backup and recovery plan to ensure that registry data can be restored in the event of a disaster.
  - This will include regular backups of the registry database and other critical data, stored in geographically diverse locations.
- **Disaster Recovery Site:**
  - disaster recovery site in a geographically separate location from primary data centers to be set up as a hot standby.
- **Recovery Time Objective (RTO) and Recovery Point Objective (RPO):**
  - Clear RTO and RPO objectives to be defined to minimize downtime and data loss in the event of a disaster.
  - Disaster recovery plan/ planned switch should be done every 6 months.

3. Indian Language Support

Internationalized Domain Names (IDNs): Enabling Domain Name Registration in Major Indian Languages

Proposed registry platform should be designed to fully support Internationalized Domain Names (IDNs) in all major Indian languages, enabling a more inclusive and accessible internet for Indian users.

1. Platform's Support for IDNs in All Major Indian Languages:

A. **Comprehensive Language Coverage:**
   a. platform will support IDNs in all 22 scheduled languages of India, as well as other commonly used regional languages.

B. **Unicode Support:**
   a. platform will fully support Unicode standards, ensuring that all Indian language characters are accurately represented and processed.

C. **Language-Specific Validation:**
   a. Platform will incorporate language-specific validation rules to ensure that IDNs are registered according to the correct character sets and linguistic conventions.

D. **Localized User Interfaces:**
   a. user interfaces for registrars and end-users will be localized to support IDNs in Indian languages.

E. **Localized Customer Support:**
   a. customer support in multiple Indian languages to assist users with IDN registration and management should be a part of the support engagement.

2. Handling Encoding and Decoding of IDN Characters:

A. **Punycode Encoding:**
   a. platform will utilize Punycode encoding to convert IDN characters into ASCII strings for DNS resolution.

B. **IDNA Standards Compliance:**
   a. platform will comply with the latest IDNA (Internationalized Domain Names in Applications) standards, ensuring accurate encoding and decoding of IDN characters.

C. **Automatic Encoding and Decoding:**
   a. system will automatically encode and decode IDN characters, simplifying the registration and management process for users.

D. **Character Set Mapping:**
   a. platform will maintain accurate character set mappings for all supported Indian languages, ensuring correct conversion between Unicode and Punycode.

E. **Validation of Input:**
   a. Input from the user, when they enter a domain name, will be validated to ensure it follows the IDN standards.

3. Localized User Interfaces: Providing an Intuitive and Accessible Experience for Indian Users

proposed registry platform will feature localized user interfaces (UIs) for both registrars and end-users, ensuring an intuitive and accessible experience in major Indian languages.

1. Platform's Provision of Localized User Interfaces for Registrars and End-Users in Indian Languages:

A. **Complete UI Localization:**
   a. All user interface elements, including menus, buttons, forms, messages, and help documentation, will be localized into major Indian languages.

B. **Language Selection:**
   a. Users will be able to select their preferred language from a dropdown menu or through browser language detection.

C. **Right-to-Left (RTL) Support:**
   a. platform will fully support right-to-left (RTL) languages, such as Urdu, ensuring proper display and functionality.

D. **Contextual Help and Documentation:**
   a. Contextual help and documentation will be provided in localized languages, guiding users through the platform's features and functionalities.

E. **Localized Error Messages and Notifications:**
   a. Error messages and notifications will be localized to provide clear and actionable feedback to users in their preferred language.

F. **Consistent Terminology:**
   a. We will maintain consistent terminology across all localized interfaces to ensure clarity and avoid ambiguity.

G. **Input Method Support:**
   a. The UI will support input methods for the Indian languages, to allow users to easily enter their desired information.

2. Experience in Developing Multilingual Applications:

Bidder should have a proven track record in developing and deploying

a. multilingual applications for diverse audiences providing examples of successful projects demonstrating expertise in localization.

A. **Localization Expertise:**
   b. a team of localization experts with experience in Indian languages and cultural nuances to be deployed on site with NIXI team.

B. **Localization Tools and Technologies:**
   a. utilize industry-standard localization tools and technologies to streamline the localization process and ensure high-quality translations.

C. **Global Best Practices:**
   a. Bidder to follow global best practices for localization, ensuring approach is efficient, effective, and scalable.

Localized Customer Support: Ensuring Accessible and Effective Assistance in Indian Languages

1. Plan for Providing Customer Support in Indian Languages:

A. **Multilingual Support Team:**
   a. Bidder to establish a dedicated multilingual support team with native speakers of major Indian languages.
   b. This team will be trained to provide technical support, address inquiries, and resolve issues in users' preferred languages.

B. **Multiple Support Channels:**
   a. support to be provided through multiple channels, including:
      1. Phone support in Indian languages.
      2. Email support in Indian languages.
      3. Live chat support in Indian languages.
      4. Online help documentation and FAQs in Indian languages.
      5. Support forums in Indian languages.

C. **Language-Specific Support Hours:**
   a. offer support during extended hours, and ensure that support in major Indian languages is available during peak usage times.

D. **Tiered Support Structure:**
   a. a tiered support structure, with initial support provided by general support agents and escalated to language-specific specialists as needed should be provided.

E. **Knowledge Base and Self-Service Resources:**
   a. Bidder to develop a comprehensive knowledge base and self-service resources in Indian languages, empowering users to find answers to common questions.

F. **Ticket Management System:**
   a. A ticket management system that allows for language designation, to ensure that tickets are routed to the correct language speaking agents should be implemented.

2. Team's Language Skills and Experience:

A. **Native Language Proficiency:**
   a. support team will consist of native speakers of major Indian languages, ensuring accurate and culturally sensitive communication.

B. **Technical Expertise:**
   a. Support agents will possess strong technical expertise in domain name registration, DNS management, and other relevant areas.
   b. They will be trained to handle technical inquiries and resolve complex issues.

C. **Customer Service Training:**

   a. The support team will receive comprehensive customer service training, emphasizing empathy, communication skills, and problem-solving abilities.
   b. They will be trained to handle diverse customer interactions with professionalism and respect.

D. **Cultural Sensitivity:**
   a. support team will be trained in cultural sensitivity, to ensure that they are aware of, and respectful of, the many cultures within India.

KYC Verification

Integration with KYC Providers: Ensuring Secure and Compliant Identity Verification for Domain Registrants

Proposed registry platform will integrate seamlessly with authorized KYC (Know Your Customer) providers in India, ensuring secure and compliant identity verification for domain registrants.

1. Platform's Integration with Authorized KYC Providers in India:

A. **API Integration:**
   a. platform will integrate with authorized KYC providers in India through secure APIs enabling real-time verification of registrant identity using data from trusted sources.

B. **Support for Multiple KYC Providers:**
   a. platform will be designed to support integration with multiple KYC providers, allowing NIXI to choose the most suitable providers based on their requirements.

C. **Data Security and Privacy:**
   a. robust security measures to be implemented to protect sensitive KYC data transmitted between our platform and the KYC providers.

D. **Compliance with Regulatory Requirements:**
   a. platform will ensure compliance with all relevant regulatory requirements for KYC verification in India.

E. **Secure Data Handling:**
   a. Bidder to ensure that data from the KYC providers is handled securely, and only used for the purpose of verifying the registrant.

F. **Consent Management:**
   a. consent management features to be built in, to allow the registrants to easily provide consent for their data to be used in the KYC process.

2. KYC Verification Process and Integration into the Domain Registration Workflow:

A. **KYC Verification Trigger:**

   a. The KYC verification process will be triggered during the domain registration process, typically after the registrant provides their personal information.

   b. This could also be triggered during a transfer of a domain name.

B. **Data Submission:**

   a. The registrant's personal information will be securely transmitted to the chosen KYC provider through the API.

C. **Real-Time Verification:**

   a. The KYC provider will verify the registrant's identity using their database and verification algorithms.

   b. This will typically involve matching the registrant's information against government databases or other trusted sources.

D. **Verification Result:**

   a. The KYC provider will return a verification result to our platform, indicating whether the registrant's identity has been successfully verified.

E. **Registration Completion:**

   a. If the verification is successful, the domain registration process will proceed.

   b. If the verification fails, the registrant will be prompted to provide additional information or contact customer support.

F. **Verification Status Logging:**

   a. The verification status will be logged in the registry database, along with the timestamp and provider information.

   b. This will provide an audit trail and ensure accountability.

G. **User-Friendly Interface:**

   a. The KYC verification process will be integrated into a user-friendly interface, ensuring a seamless experience for registrants.

   b. We will provide clear instructions and guidance throughout the process.

H. **Automated Process:**

   a. The entire KYC verification process will be automated, minimizing manual intervention and reducing the risk of errors.

I. **Error Handling:**

   a. The system will have robust error handling, to deal with the inevitable errors that will occur during the KYC process.

J. **Retry Logic:**

   a. There will be retry logic, to deal with temporary errors from the KYC provider.

Data Security and Privacy: Ensuring the Confidentiality and Integrity of Sensitive KYC Information

proposed registry platform is to be designed with a strong emphasis on data security and privacy, particularly concerning the protection of sensitive KYC (Know Your Customer) data.

1. Platform's Security Measures to Protect Sensitive KYC Data:

1. **Data Encryption at Rest and in Transit:**
   a. All sensitive KYC data will be encrypted both at rest within our database and during transmission between our platform and KYC providers.

   b. industry-standard encryption algorithms, such as AES-256 and TLS 1.3, to be used to ensure data confidentiality.
2. **Access Control and Authorization:**
   a. strict access control mechanisms to limit access to KYC data to authorized personnel only to be implemented.
   b. Role-based access control (RBAC) to be used to define granular permissions based on job responsibilities.
   c. Multi-factor authentication will be implemented.
3. **Data Minimization:**
   a. W principle of data minimization to be adhered to , collecting only the necessary KYC data required for verification purposes.
4. **Secure Data Storage:**
   a. KYC data will be stored in secure, isolated databases with robust security measures, including firewalls, intrusion detection systems, and regular security audits.

5. **Data Retention Policies:**
   a. clear data retention policies for KYC data to be established, specifying the duration for which data will be stored and the procedures for its secure deletion and compliance with legal retention periods to be ensured.
6. **Regular Security Audits and Vulnerability Assessments:**
   a. regular security audits and vulnerability assessments to identify and address potential security weaknesses to be conducted.
   b. This will include penetration testing and security code reviews.

7. **Secure API Integrations:**
   a. All API integrations with KYC providers to be secured using industry best practices.
   b. This will include authentication, authorization, and data encryption.
8. **Logging and Monitoring:**
   a. comprehensive logging and monitoring systems to be implemented to track access to KYC data and detect any suspicious activity.
   b. This will enable us to quickly identify and respond to security incidents.

2. Compliance with Relevant Data Privacy Regulations in India:

A. **Information Technology Act, 2000 (IT Act):**
    a. provisions of the IT Act, including Section 43A, which addresses data protection and security to be complied with.
    b. W reasonable security practices and procedures to protect sensitive personal data to be implemented.

B. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules):**
    a. SPDI Rules to be adhered to , which specify the requirements for handling sensitive personal data or information.

    b. This will include obtaining consent, providing privacy notices, and implementing security safeguards.

C. **Digital Personal Data Protection Act, 2023:**
    a. all regulations laid out in the Digital Personal Data Protection Act, 2023 to be adhered to. This includes obtaining consent, data principals rights, and cross border data transfer rules and any other applicable clause.

D. **Data Localization:**
    a. all data localization rules set forth by the Indian government to be adhered to .

E. **Data Principal Rights:**
    a. implement systems that allow the data principals to exercise their rights, such as right to correction, right to erasure, and right to grievance redressal.

F. **Consent Management:**
    a. implement a robust consent management system to obtain explicit consent from users for the collection and processing of their KYC data.

G. **Privacy Policy:**
    a. develop a clear and comprehensive privacy policy that explains our data collection, use, and disclosure practices.
    b. This policy will be made readily available to users in Indian languages.

H. **Data Breach Notification:**
    a. procedures for notifying users and relevant authorities in the event of a data breach, to be established and bidder to comply with the notification requirements outlined in Indian data privacy regulations.

I. **Regular Compliance Audits:**
    a. regular compliance audits to be conducted to ensure that data security and privacy practices align with Indian data privacy regulations.
    b. Bidder to stay up to date on all new and changing regulations.

Compliance with Regulatory Requirements: Ensuring Adherence to Indian KYC Regulations in Domain Registration

proposed registry platform to be designed with a deep understanding of the regulatory requirements for KYC (Know Your Customer) verification in the domain registration process within India.

1. Understanding of Regulatory Requirements for KYC Verification in Domain Registration:

A. **RBI Guidelines on KYC:**
   a. Reserve Bank of India (RBI) guidelines on KYC, which establish the framework for customer identification and due diligence to be understood by the bidder while designing the platform capabilities.

B. **Prevention of Money-Laundering Act, 2002 (PMLA):**
   a. Bidder to acknowledge the relevance of the PMLA, which mandates KYC verification for certain transactions to combat money laundering and .
   ensuring that the platform aligns with the PMLA's requirements for customer identification and record-keeping.

C. **Information Technology Act, 2000 (IT Act) and Related Rules:**
   a. Bidder to recognize the IT Act's provisions concerning data security and privacy, which are crucial for protecting KYC information and adhere to
   Digital Personal Data Protection Act, 2023 regulations.

D. **Indian Domain Name Policy:**
   a. Bidder to understand and comply with specific regulatory requirements pertaining to domain name registration in India, including any mandates for registrant verification.

E. **Telecom Regulatory Authority of India (TRAI) Regulations:**
   a. While not directly related to all domain names, bidder to be aware of TRAI regulations that may, in some cases, intersect with domain registration, especially regarding contact information.

F. **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016:**
   a. Bidder to be aware of the Aadhaar Act and its implications for identity verification, while remaining cognizant of the limitations imposed by the supreme court.

G. **Video KYC regulations:**
   a. Bidder to be aware of the RBI video KYC regulations, and how they can be used to augment the KYC process.

2. Platform's Measures to Ensure Compliance:

A. **Integration with Authorized KYC Providers:**
   a. Platform will integrate with authorized and RBI-compliant KYC providers in India, ensuring that verification is conducted through trusted channels.

    b. This will ensure that the KYC process adheres to established regulatory standards.

B. **Data Security and Privacy Measures:**
    a. robust data security and privacy measures to protect KYC information, as detailed in the previous section to be implemented.

C. **Audit Trails and Record-Keeping:**
    a. platform will maintain comprehensive audit trails and records of all KYC verification activities to
    facilitate regulatory audits and ensure accountability.

D. **Regular Compliance Audits:**
    a. regular compliance audits to ensure that our KYC verification processes remain aligned with evolving regulatory requirements, to be conducted.
    b. This will involve (though not limited to) reviewing procedures and systems to identify and address any compliance gaps.

E. **Policy Updates and Training:**
    a. procedures for monitoring and implementing updates to KYC regulations To be established.
    b. Our team will receive regular training on KYC compliance requirements.

F. **Clear Consent Mechanisms:**
    a. Bidder to ensure that registrants provide explicit consent for their KYC data to be collected and used for verification purposes.
    b. This will adhere to data privacy principles and regulatory requirements.

G. **Secure Data Transmission and Storage:**
    a. secure data transmission protocols and storage methods to safeguard sensitive KYC information to be utilized.

H. **Reporting of Suspicious Transactions:**
    a. mechanisms for reporting suspicious transactions related to domain registration, as required by the PMLA to be implemented.

Implementation & Deployment

Project Management: Ensuring Efficient and Successful Implementation of the Registry Platform

proposed registry platform implementation will be managed using a robust and proven project management methodology, ensuring efficient execution, timely delivery, and adherence to NIXI's requirements. clear communication, proactive risk management, and meticulous planning methodologies to be followed.

1. Project Management Methodology and Approach:

A. **Agile and Iterative Approach:**

    a. an agile and iterative approach, allowing for flexibility and adaptability throughout the project lifecycle, to be followed.

B. **Dedicated Project Team:**
    a. W a dedicated project team with experienced project managers, developers, testers, and subject matter experts to be assembled.
    b. This team will be responsible for all aspects of the project, from planning and design to implementation and deployment.

C. **Clear Communication and Collaboration:**
    a. clear and consistent communication with NIXI to be prioritized, ensuring that all stakeholders are informed and involved throughout the project.
    b. regular meetings, progress reports, and communication channels to facilitate collaboration to be established/conducted.

D. **Risk Management:**
    a. A proactive risk management process to identify, assess, and mitigate potential risks, to be implemented.
    b. This will include developing contingency plans and regularly monitoring risks throughout the project lifecycle.

E. **Quality Assurance:**
    a. adherence to rigorous quality assurance standards to ensure that the registry platform meets NIXI's requirements and performs reliably.
    b. This will include thorough testing, code reviews, and user acceptance testing.

F. **Change Management:**
    a. A robust change management system, that allows for changes in the project, while still maintaining the project timeline to be in place.

G. **Documentation:**
    a. Detailed documentation throughout the project to be maintained.

2. Key Considerations:

A. Regular progress reports and status updates will be provided to NIXI throughout the project.
B. Flexibility will be maintained to accommodate any changes or adjustments to the project scope.
C. A dedicated communication channel will be established for prompt resolution of issues and concerns.
D. All milestones will be documented and signed off on by the relevant parties.

Data Migration: Ensuring Seamless and Accurate Transfer of Existing Registry Data

The proposed data migration plan to be designed to ensure a seamless, secure, and accurate transfer of existing registry data to the new platform.

A. Plan for Migrating Existing Registry Data to New Platform:

B. Bidder to detail out plan with milestones and approach for the migration activity benchmarking against global standards.

Training and Support: Ensuring a Seamless Transition and Ongoing Operational Success

Proposed plan for training and support to be designed to ensure a smooth transition to the new registry platform and provide ongoing assistance to NIXI staff and registrars.

1. 2. Ongoing Support and Maintenance Services:

A. **Dedicated Support Team:**
   a. A dedicated support team with expertise in registry platform operations and troubleshooting to be provided.
   b. This team will be available to respond to inquiries and resolve issues promptly.

B. **Multiple Support Channels:**
   a. support through multiple channels to be provided, including:
      i. 24/7 phone support.
      ii. Email support.
      iii. Live chat support.
      iv. Online ticketing system.
      v. Knowledge base and FAQs.

C. **Service Level Agreements (SLAs):**
   a. clear SLAs for response times and resolution times, ensuring timely support to be established

D. **Proactive Monitoring and Maintenance:**
   a. proactive monitoring and maintenance procedures to identify and address potential issues before they impact operations to be implemented.
   b. This will include regular system health checks, performance monitoring, and security audits.

E. **Regular System Updates and Enhancements:**
   a. regular system updates and enhancements to be provided to ensure that the platform remains up-to-date and secure.
   b. This will include bug fixes, security patches, and new feature releases.

F. **Knowledge Base and Documentation:**
   a. a comprehensive knowledge base and documentation library to be maintained, that is easily searchable.

G. **Performance Optimization:**

   a. Bidder to continuously monitor the performance of the system and make optimizations as needed.

H. **Security Updates:**

   a. ensure that all security updates are applied in a timely manner.