GOVERNMENT OF KERALA

Abstract

Planning and Economic Affairs (RKI) Department- Setting up of a Unified Registry for the State of Kerala – Establishment of an Aadhaar Vault as part of the First Phase of the project at an estimated cost of ₹26.29 crore – Administrative Sanction accorded – Orders issued.

PLANNING & ECONOMIC AFFAIRS (RKI) DEPARTMENT

G.O.(Rt)No.466/2021/P&EA Dated,Thiruvananthapuram, 03/11/2021

Read: 1. G.O. (P) No. 16/2018/P&EA dated 09/11/2018.

2. G.O. (Ms) No. 26/2021/P&EA dated 03/09/2021.

3. Letter No.KSITM/Dir/2021 dated 25/10/2021 from the Director, KSITM.

ORDER

As per G.O. read 1st above, in-principle sanction was accorded for setting up of a Unified Registry for the State. The project is intended to improve the effectiveness & efficiency of Social Welfare Schemes of Kerala through establishment of a centralized common platform for beneficiary identification and selection, enhancement of transparency and effectiveness of beneficiary selection process, consolidation and de-duplication of data and providing a safety net from disasters both, ex ante in prevention and mitigation from the impact of a disasters and ex poste, to cope with the impact of natural disasters etc. As a part of this initiative, the Government also accorded sanction to establish an 'Aadhaar Vault' along with the attendant hardware, software, and manpower requirements, under the Rebuild Kerala Initiative, at an estimated cost of ₹34.32 crore.

2. The Director, Kerala State Information Technology Mission (KSITM), as per letter read 3rd above, has subsequently submitted a proposal for establishing an Aadhaar Vault which serves a mandatory centralized repository for all Aadhaar numbers/VIDs collected by the Government departments [which act as the sub- Authentication User Agencies (AUA) in this case, as per the definition of Unique Identification Authority of India (UIDAI)] for specific purposes under the Aadhaar (Targeted Delivery Of

Financial and Other Subsidies, Benefits and Services) Act, 2016 as amended by Aadhaar and Other Laws (Amendment) Act, 2019.

3. The Government, after having considered the proposal in detail, are pleased to accord Administrative Sanction for the "Establishment of an Aadhaar Vault" at an estimated cost of **₹26.29 crore (Rupees Twenty-six crore and Twenty-nine lakh only)**, as a part of the First Phase of setting up of a Unified Registry for the State of Kerala, under the Rebuild Kerala Initiative. The technical details ,financial parameters and the time lines for implementation of the project will be as detailed in the **Annexure** to this G.O. The expenditure in this regard will be debited to the budget provision under H/A 5475-00-115-94-Post flood Projects under Rebuild Kerala Initiative (P).

4. All procurement as part of implementation of the work shall be done in a fair and transparent manner in accordance with the extant rules, and all mandatory clearances from relevant departments shall be obtained wherever applicable.

(By order of the Governor)
Rajesh Kumar Singh I A S
Additional Chief Secretary

To:
Additional Chief Secretary, Finance Department
Principal Secretary, Electronics & Information Technology Department.
Director, Kerala State Information Technology Mission.
The Principal Accountant General (A&E/Audit), Thiruvananthapuram.
Finance Department.
Information & Public Relations (Web & New Media) Department (for publishing in Government website).
Stock File/ Office Copy [F.No.RKI1/47/2021-PLGEA].

Forwarded /By order

Section Officer

ANNEXURE

SALIENT FEATURES OF THE AADHAAR VAULT

I. Introduction:

Aadhaar Vault is a centralized repository for all Aadhaar numbers/VIDs collected by the government departments (sub- AUA) for specific purposes under Aadhaar Act and Regulation, 2016. A global AUA authorized to store Aadhaar numbers must mandatorily implement an Aadhaar vault solution as per circular 11020/205/2017 dated 25/07/2017. The Government of Kerala desire to establish a Government wide Aadhaar vault to manage Aadhaar specific authorization in respect of social security scheme benefit management as well as schemes for which Aadhaar is mandatory. Each beneficiary will be identified by a SmartID against the Aadhaar number. However there is no direct link between Smart ID and Aadhaar number. The SmartID and Aadhaar number pair will be stored in the Aadhaar vault in encrypted form along with key management system using HSM or software HSM. The Aadhaar vault and the HSMwill be secured with suitable security protocols.

Aadhaar vault is a highly secure Aadhaar data management solution that is independent and isolated from the applications that use the Aadhaar number using secured APIs. The objective of Aadhaar vault is to reduce the footprint of Aadhaar numbers within the department applications and environments to reduce the risk of unauthorized access.

II. Key Features

- Encryption of Aadhaar number, Virtual ID of the data of citizens.
- Use of a hardware based cryptographic store for management of encryption keys.
- Implementation of key rotation schedules and key versioning.
- Access control, authorization and policy management.
- Support for access based on Smart ID, UID token or department wise reference key aliases.
- Versioning of e-KYC responses for tracking historical changes to Aadhaar records.
- REST API based access to authorized vault operations.
- Support for pushing domain specific custom attributes from department

- Support for pushing domain specific custom attributes from department applications to the vault Database (DB).
- Support applications of multiple government departments
- Aadhaar vault and HSM implemented on isolated bare metal hardware.
- Isolation of hardware and software components in a separate militarized zone with segment VLAN.
- Physical security for Aadhaar vault /HSM zone with industry standard access control
- Monitoring and logging provisions that is compliant to UIDAI requirements.
- Isolated central administration console for management and privileged vault access.

III. Architecture

Aadhaar Vault comprises of hardware and software components to create a secure and UIDAI compliant vault solution. The major components of the architecture are given below:

1. **Vault VLAN:-** an independent and isolated network consisting of the application and DB servers that implements the Aadhaar vault. The access to vault VLAN is allowed only from authorized application servers of various departments.

2. **Vault DB :-** The database for Aadhaar vault is a No SQL/SQL database designed to allow Aadhaar and e-KYC data from multiple departments to coexist. The key fields like Aadhaar/VID and demographic details would be encrypted in column level before it is stored in the DB. The vault DB is secured since it only contains reference keys and encrypted data, and this makes it safe for BCP. The vault DB shall also support versioning of e-KYC data of an Aadhaar number. This allows department applications to trace back and link to an old version of e-KYC data for an Aadhaar number.. The vault DB shall allow departments to store domain specific metadata against an Aadhaar number. These metadata access may be granted to any other authorized departments to securely consume those attributes.

3. **Audit DB :-** The audit DB is a No SQL audit trail DB that records the API activities like storing Aadhaar e-KYC data, fetching Aadhaar or e-KYC data by the reference key, metadata access etc. The Vault API provides access to the vault DB. The encryption and decryption of

sensitive data fields is done by the vault API. The requests from registered departments shall be authenticated by verifying the HMAC send in the request header. The HMAC key would be pre-shared with the department on granting access to the vault. The vault API access is restricted by IP whitelisting at both API and network level. In the API level, a set of allowed IPs for each department is maintained and verified to grant access. The vault API communication channel is secured using mutual TLS authentication. The sensitive fields like Aadhaar and demographic details are encrypted using AES256 using the vault HSM before storing in vault DB. Similarly, the encrypted data from vault DB is decrypted by the API before returning to the requesting application.

4. **Vault HSM**:- Vault HSM is a hardware appliance used to securely store and manage the cryptographic keys and operations required by the vault API. It provides cryptofunctions to vault API for encryption and hashing of sensitive data. It must be implemented using a dedicated server in an isolated VLAN (separate from the Aadhaar vault). Multiple HSM appliances must be clustered to ensure availability of HSM services. The key store may be generated within one HSM and replicated to all other HSM within the cluster. Vault HSM can also be implemented as software based crypto processing service. A software HSM solution secures cryptographic keys in a PKCS#11 token store. A software based HSM requires custom implementation of Crypto service APIs, management console and key management.

   (i) Crypto Service APIs :- A set of high-level REST APIs that are deployed in HSM Server to enable secured communication from vault APIs to PKCS#11 key stores in HSM server. The vault API consumes the HSM Service APIs for encryption and decryption operations. The HSM VLAN is secured by isolating it as a separate VLAN to prevent access to token files. The HSM VLAN must be allowed access only from the Vault API server.

   (ii) HSM Management Console :- An HSM appliance must implement industry-standard policies for key rotation, key scheduling, and key versioning. The HSM management console is an administration app used to manage the key management activities like periodic rotation of master keys and derived keys.

   (iii) Key Management:- The HSM service must support a key management protocol for key generation, encryption, key storage, and decryption. Sensitive data fields in Aadhaar data vault must be encrypted using symmetric key cryptography. The symmetric keys must

be periodically rotated to ensure compliance in management of cryptographic keys. The following scheme may be used:

(a) Initialization:- An asymmetric key pair is generated in the PKCS#11key store of the HSM.The key store file is replicated to all the HSM nodes. This key is called the Key Encryption Key (KEK) as it is used to encrypt the data encryption keys. A random symmetric key called the Data Encryption Key (DEK) needed for encryption of actual data. The crypto service generates a DEK using the HSM. The DEK is encrypted using KEK and stored in the key management DB along with a key identifier (KID) and version. The KID is configured withAadhaar vault service to be used for encryption

(b) Encryption:-

i) Aadhaar vault API submits sensitive data and key identifier (KID) to cryptoservice API for encryption.

ii) Cryptoservice uses DEK to encrypt the data and returns the cipher text along with the key identifier and key version.

iii) The cipher text along with the KID and key version are stored in DB.

(c) Decryption:-

i) Aadhaar vault API reads the cipher text from vault DB along with the key identifier (KID) and the version.

ii) The cipher text, KID and key version are submitted to crypto API for decryption.

iii) Crypto API reads the encrypted DEK and based on the KID and key version.

iv) Encrypted DEK is decrypted by submitting it to the HSM.

v) Plain DEK is used to decrypt the cipher text and return it back to the Aadhaar vault API.

(d) Key Rotation:- Key rotation is the process of generating and replacing a new DEK for an existing key identifier (KID). Key rotation must be done once in 6 months.The newly generated key would be identified using the same KID but with an incremented version number. The HSM management console is used for key rotation. The latest version of a key identifier will be used for all future encryption requests

after key rotation.

5. Vault Management Console:- The Vault Management Console (VMC) is a web based Aadhaar vault management tool accessible only from a single authorized client to provision the following:

1. On-boarding department applications toAadhaar vault
2. Generating HMAC keys forAPI access
3. Whitelisting IPs for API access
4. RBAC management
5. Accessing activity audit trail records
6. Monitoring Aadhaar vault operations

IV. Aadhaar Vault – Implementation Requirements

- Dedicated physical server isolated from other networks in a militarized zone.
- Backup server in the same type of environment as live server.
- Dedicated network devices
- A robust database to keep the Aadhaar in encrypted forms along with the reference Keys, and provision to store Audit Log/Request/Response XML and Audit trails Including user Consent
- A robust key management system for the generation of the reference key.
- Bulk Transformation Utility that converts existing ADHAAR number into Reference Keys and vice versa is required and needs to be developed.

V. Technical Specifications of Hardware Security Module (HSM)

1. Regulatory compliance to FIPS 140-2 Level 3
2. Memory within HSM – Minimum of 8 MB
3. Number of partitions within HSM – 5 or higher expandable to 10 logical partitions including licenses
4. Key storage Area – Inside HSM
5. Should support Key storage capacity (inside HSM) of 9000 or higher keys for RSA 2048 bit, triple DES, AES 128-256 bit

6. Signing speed in Transactions per second - RSA 2048 bit/AES 255 bit Signing performance – 5000 or higher

7. Key Generation Speed – Number of keys generated per second – 10 or higher

8. Should support for Random Number Generation

9. HSM should support Application Programming Interfaces (APIs) viz PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG.

10. Should support audit and logging

11. HSM to be configured in High Availability (HA) mode

12. Should support clustering and load balancing.

13. Less than 30 seconds for key replication across the cluster.

14. Should support cryptographic separation of application keys using logical Partitions.

15. Should support multi-factor authentication.

16. Minimum Dual Gigabit Ethernet ports (to service two network segments)

17. HSM should support IPv4 & IPv6.

18. Supported Cryptographic Asymmetric algorithms: RSA (2048-8192), DiffieHellman, DSA, KCDSA, ECDSA, ECDH, ECIES.

19. Supported Cryptographic Symmetric algorithms: AES, ARIA, CAST, HMAC, SEED, Triple DES, DUKPT, BIP32.

20. Supported Functionality – 3 DES, DUKPT, Master/Session, TR-31, RSA, ATM, EMV Encryption/Decryption/Signing

21. Form factor – 1U rack mountable

22. HSM should support cryptographic offloading and acceleration.

23. HSM should provide Authenticated multi-role access control.

24. HSM should have strong separation of administration and operator roles.

25. Should have secure key wrapping, backup, replication and recovery.

26. Safety and environmental compliance - Compliance to UL, CE, RoHS2, WEEE.

27. Management and monitoring

i. Support Remote Administration —including adding applications, updating firmware, and checking the status— from NoC.

ii. Syslog diagnostics support.

iii. Command line interface (CLI)/graphical user interface (GUI).

iv. Support SNMP monitoring agent.

28. Should have the ability to backup keys, replicate keys, store keys in offline locker facilities for DR. The total capacity is in line with the total number of keys prescribed.

29. On site OEM warranty for 5 years and OEM support maintenance for another 5 years.

VI. Detailed Specification of Servers and other hardware for Aadhaar Vault at State Data Centre

Sl. No.	Item description	Qty (No.s)
	Hardware	
1.	**Database Servers**	
	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher OR 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 1 TB RAM DDR4 SDRAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with 15m LC-LC OFC, Network Controller- Minimum Six ports- 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF from OEM to be submitted, 5 year on site OEM warranty.	2
2.	**Server for creating VM's for App Servers, Testing Servers, Demo Servers**	

	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher or 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 2 TB RAM DDR4 SDRAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480 GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with15m LC-LC OFC, Network Controller- Minimum Six ports - 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF form OEM to be submitted, 5 year onsite OEM warranty.	2
	Rack mountable (1U) 8 Port KVM Switch supporting PS/2 /USB interface for keyboard & mouse with OSD, cables and accessories to connect all ports.	1
	42" U Rack	1
3.	**SAN**	
	50 TB SAN Storage (raw), scalable to 100 TB with SSD – 20 TB (expandable to 40 TB) and SAS – 30 TB (expandable to 60 TB), Dual controller with RAID Level Support 5,6,10 configured in HA, Hot swappable redundant power supplies, Must be able to add additional disks on the fly Minimum of Dual controller in active-active mode scalable to four controllers, Ports – 4 x 16 Gbps FC or higher ports, 8x 12 Gbps or higher SAS host ports, Minimum of 64 GB controller based configurable cache and should be scalable to 128 with 72 hrs battery backup or equivalent mechanism for cache data protection.	1
4.	**Software**	
	RHEL Enterprise Edition (Latest with 5 Year Support)	License required for all the above servers in Sl.No .1 and 2

	RHEV (latest with 5 Year Support)	License required for creating VM 's as per Sl.No. 2 above.

VII. Detailed Specification of Servers and other hardware for Aadhaar Vault at Far DR.

Sl. No.	Item description	Qty (No.s)
	Hardware	
1.	**Database Servers**	
	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher OR 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 512 TB RAM DDR4 SD RAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with 15m LC-LC OFC, Network Controller- Minimum Six ports- 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF from OEM to be submitted, 5 year on site OEM warranty.	2
2.	**Server for creating VM's for App Servers, Testing Servers, Demo Servers**	

	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher or 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 1 TB RAM DDR4 SD RAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480 GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with 15m LC-LC OFC, Network Controller- Minimum Six ports - 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF form OEM to be submitted, 5 year onsite OEM warranty.	1
	Rack mountable (1U) 8 Port KVM Switch supporting PS/2 /USB interface for keyboard & mouse with OSD, cables and accessories to connect all ports.	1
	42" U Rack	1
3.	**SAN**	
	50 TB SAN Storage (raw), scalable to 100 TB with SSD – 20 TB (expandable to 40 TB) and SAS – 30 TB (expandable to 60 TB), Dual controller with RAID Level Support 5,6,10 configured in HA, Hot swappable redundant power supplies, Must be able to add additional disks on the fly Minimum of Dual controller in active-active mode scalable to four controllers, Ports – 4 x 16 Gbps FC or higher ports, 8x 12 Gbps or higher SAS host ports, Minimum of 64 GB controller based configurable cache and should be scalable to 128 with 72 hrs battery backup or equivalent mechanism for cache data protection.	1
4.	**Software**	
	RHEL Enterprise Edition (Latest with 5 Year Support)	License required for all the above servers in Sl.No. 1 and 2

	RHEV (latest with 5 Year Support)	License required for creating VM 's as per Sl.No. 2 above.

VIII. Detailed Specification of Servers and other hardware for Aadhaar Vault at Near DR.

Sl. No.	Item description	Qty (No.s)
	Hardware	
1.	**Database Servers**	
	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher OR 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 512 TB RAM DDR4 SD RAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with 15m LC-LC OFC, Network Controller- Minimum Six ports- 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF from OEM to be submitted, 5 year on site OEM warranty.	2
2.	**Server for creating VM's for App Servers, Testing Servers, Demo Servers**	

	Rack Mount Server – 4 nos. Intel Xeon 3rd generation with 20 core or higher or 2 nos. of EPYC AMD processor with 40 core or higher, 2.3 GHz or higher base frequency with 1 TB RAM DDR4 SD RAM with ECC, 1.4 TB or higher SAS SSD drives with 3x480 GB or higher capacity drives, 12 Gbps RAID redundant Controllers with 2 GB cache for RAID 0 1 5, Dual 16 GBPS or higher FC Ports on two different controllers HBA with 15m LC-LC OFC, Network Controller- Minimum Six ports - 4x10 GBPS (dual port each on separate controllers) populated with SFP+ with necessary DAC and 2x10 Gbps, Hot swappable redundant power supplies, MAF from OEM to be submitted, 5 year onsite OEM warranty.	1
	Rack mountable (1U) 8 Port KVM Switch supporting PS/2 /USB interface for keyboard & mouse with OSD, cables and accessories to connect all ports.	1
	42" U Rack	1
3.	**SAN**	
	50 TB SAN Storage (raw), scalable to 100 TB with SSD – 20 TB (expandable to 40 TB) and SAS – 30 TB (expandable to 60 TB), Dual controller with RAID Level Support 5,6,10 configured in HA, Hot swappable redundant power supplies, Must be able to add additional disks on the fly Minimum of Dual controller in active-active mode scalable to four controllers, Ports – 4 x 16 Gbps FC or higher ports, 8x 12 Gbps or higher SAS host ports, Minimum of 64 GB controller based configurable cache and should be scalable to 128 with 72 hrs battery backup or equivalent mechanism for cache data protection.	1
4.	**Software**	
	RHEL Enterprise Edition (Latest with 5 Year Support)	License required for all the above servers in Sl.No. 1 and 2

	RHEV (latest with 5 Year Support)	License required for creating VM 's as per Sl.No. 2 above.

IX. Human Resource requirement for the Vault

Designation	Qualification & Experience	Roles & Responsibilities	Salary (per month) (₹)	Total cost (₹)

System & DB Admin – 1 No.	B. Tech or MCA or equivalent; 5 years and above	• Installing, configuring, maintaining and monitoring of RHEL/Ubuntu Servers • Installing, configuring, maintaining and monitoring of JBoss, Tomcat Servers. • Basic network administration and configuration • Provide consultancy services to function and customers • Ensuring server security and monitoring the server logs • Work with customer infrastructure and fix issues remotely • Ability to work independently • Communicating to users and management • Implement and maintain policies, procedures, and standards to ensure data security and integrity of test and production data • Managing and monitoring enterprise level database. • Managing database backups and recovery planning • Uploading data into databases • Ensuring database security and monitoring database logs.	60,000	14,40,000

Security and Network Admin-1 No.	B. Tech or MCA or equivalent 5 years and above	• Installing, administering, and troubleshooting network security solutions. • Updating software with the latest security patches and ensuring that proper defences are present for each network resource. • Performing vulnerability and penetration tests, identifying and defending against threats, and developing disaster recovery plans. • Configuring security systems, analyzing security requirements, and recommending improvements. • Monitoring network traffic for suspicious behavior. • Creating network policies and authorization roles and defending against unauthorized access, modifications, and destruction. • Consulting with staff, managers, and executives about the best security practices and providing technical advice. • Configuring and supporting security tools, such as firewalls and anti-virus software. • Training staff to understand and use security protocols.	60,000	14,40,000
Project Engineer- 1	B.E/B. Tech (Electronics/Compute	• Will be positioned at the State Data Centre for managing and monitoring the daily operation	60,000	14,40,000

No	r Science/IT) Minimum 3 years work experience in a Data Centre operated by State or Central Govt./Nationalized Banks/ Corporate Companies.	al activities, ensuring the availability of the installed systems. • Configuration change management of IT / Networking devices and software upgrades. • Maintain security, backup, and redundancy strategies • Incident management, tracking and reporting. • Tracking and management of IT and Non-IT Assets, maintaining stock register. • Conducting Information Systems Security Audits, vulnerability Assessment and Risk Assessments, mock drills for BCP/Disaster Recovery/Backup etc. • Daily Health checkup for the Cloud Servers, Storage, Backup, Network devices. • Supervision and verification of works being carried out in the State Data Centres. • Verification of Bills of Materials during purchases. • Verification of the bills towards the utility payments, consumables etc. • Co-ordinate activities for performing ISO compliance audit • Co-ordinate activities for performing TPA audit			

		• Co-ordinate with vendors, Telecom Service Providers for the timely resolution of faults. • Identification of unused assets/ resources and reporting. • Ensuring timely renewals of AMC, warranty etc.		

Technical Consultant-1 No. (6 months)	B.E/B.Tech (Electronics/Computer Science/IT) Minimum 10 years experience in managing and consulting in IT industry	• Performing analysis on hardware, software, and network capabilities. • Consulting with management and other departments as required. • Improving system efficiency by consulting with end-users and providing innovative solutions. • Analyzing and improving the performance of web-based portals. • Resolving logged errors, as well as ensuring system security and encryption. • Documenting processes and monitoring system performance metrics. • Ensuring that computer hardware remains compatible with software updates. • Implementing the latest technological advancements and solutions. • Performing diagnostic tests and troubleshooting. • Training end-users on hardware functionality and software programs.	2,50,000	15,00,000 (6 months)

Engineer – IT 2 Nos.	BE / B.Tech (CS / EC / IT) / MCA 1-2 years (with 1 year in Information Security field)	• Provide initial assistance & Administer CERT-K equipment and peripheral devices. • Undertake initial data entry and the sorting and prioritizing of incoming information and build up State Repository • Maintain the infrastructure for CERT-K products; this includes secure servers, the data. • Maintain Website & Create new Content & corresponding designs for website in conjunction with CERT-K team. • Administer Web Servers & applications. • Incident detail collection & Analysis • CMP, Training support, Tutorial creation	45000	21,60,000
System Engineer-3 Nos	B.E/B.Tech (Electronics /Computer Science/IT) Minimum two years work experience in Information Security / Cloud computing / Networking from reputed Companies/Gov	• Handling and processing the service requests for server, storage provisioning at the State Data Centre as per the prevailing policies. • Provision of resources at the Public Cloud / DR site as per requirement • Monitor and test application performance for potential bottlenecks, identify possible solutions for fixing. • Validating the hardening of the servers, security posture che	35,000	25,20,000

	ernment org anization / Banks	ck for the identification of kno wn vulnerabilities, open ports etc. • Monitoring the health and perf ormance of Network / Storage and Servers on daily basis. • Incident logging and tracking of events, Root Cause Analysi s. • Analysing reports from Third Party Audit (TPA) and taking preventive actions • Log analysis, monitoring and r eporting critical events/alarms to the State Data Centre. • Preparing daily reports on the resource utilization, network tr affic, security incidents etc. • Assisting in the preparation of Technical Specification, evalu ation of tenders • Providing technical support fo r Data Centre related queries o ver email, phone etc. • Collecting feedback from the client departments on the servi ces delivered.		

Senior System Admin – 1 No	B. Tech or MCA or equivalent 5 years and above	• Installing, configuring, maintaining and monitoring of RHEL/Ubuntu Servers • Installing, configuring, maintaining and monitoring of JBoss, Tomcat Servers. • Basic network administration and configuration • Provide consultancy services to function and customers • Ensuring server security and monitoring the server logs • Work with customer infrastructure and fix issues remotely.	60000	14,40,000

DB Admin- 1 No.	B-Tech/ MCA or equivalent 5 years and above	• Ability to work independently • Communicating to users and management • implement and maintain policies, procedures, and standards to ensure data security and integrity of test and production data • Managing and monitoring enterprise level database. • Managing database backups and recovery planning • Uploading data into databases • Ensuring database security and monitoring database logs • Basic network administration and configuration • Provide consultancy services to functions and customers • Work with customer infrastructure and fix issues remotely	80,000	19,20,000

Manager (Infrastructure)- 1 No.	B Tech in CSE/IT Minimum 8 years experience in managing large IT infra projects including networking and Data Centre. Experience in RFP, bid process management.	• Take care of all infra needs to roll out Aadhaar Vault and Unified Registry • Ensuring data security, BCP, DR for applications hosted • Application Performance Monitoring, Network Monitoring	90000	21,60,000
Project Manager- 1 No.	B.Tech in CSE/IT/ECE Minimum 5 years experience in managing IT projects. Experience in RFP, bid process management (optional)	• Interface with all departments to roll out Govt services and schemes • Interface with SDC team • Track Unified registry Aadhaar Vault project • Manage the Team	80,000	19,20,000

X. Civil/Infrastructure upgrade at SDC to accommodate the Vault

The estimated amount for State Data Centre -2 expansion activities is ₹12.27 Crore excluding taxes. As per G.O.(Rt)No.119/2021/ITD dated 25/08/2021, an amount of ₹5.25 crore is sanctioned for the year 2021-22 as the Phase-I activities (Civil/Electrical works, BMS, Networking passives etc.), and the remaining ₹7 Crore will be provided by the RKI. The expansion activities are required in view of secure hosting of the Aadhaar Vault, Unified Registry and associated services. The split up for the ₹12.27 Crore is given below.

Sl. No.	Particulars	Estimated amount (₹) excluding taxes
1.	Supply & Installation of civil & interior package of (involving flooring, ceiling, partitions, cladding, glazing,doors, furniture etc.)	55,25,000
2.	Supply & Installation of electrical package (comprising of transformer, all panels, BBTs, earthing, terminations, raceways, cable trays etc.)	2,65,00,000
3.	Supply & installation of Diesel Generator including foundation, exhaust, pumps and tanks, etc.	1,70,00,000
4.	Supply & Installation of HVAC package consisting of precision & comfort cooling	1,86,50,000
5.	Supply & Installation of safety & surveillance comprising of fire alarm and suppression systems, CCTV system, VESDA, Access control system, Data Center Information Management (DCIM), Rodent Repellent System (RRS), Water Leakage Detection (WLD) etc.	1,72,50,000
6.	Supply & Installation of UPS & Batteries	1,03,00,000
7.	Supply & Installation of Network Passives (Racks, cables, Patch Panels, IPDU, Fiber & Copper Pathways etc.)	2,25,00,000
8.	UAT & Miscellaneous expenses	50,00,000
9.	**Total**	**12,27,25,000**
	Amount required from the RKI	**7,00,00,000.00**

XI. Total Financial Outlay

Sl. No	Item	Approximate Cost (₹ crore)
1.	Hardware & Software	15.1
2.	Human Resource(to be funded from RKI for two years)	1.8
3.	Civil/Infrastructure upgrade at SDC to accommodate the Vault	7
4.	Contingency fund (10%)	2.39
	Total	**26.29**

XII. Timeline of implementation of the Vault

Sl. No.	Activities	Timelines (Months)
1.	Obtaining AS	T
2.	Recruitment of Manpower	
	Notification of recruitment	T+0.25
	Interview process	T+1.25
	Short listing and issuance of appointment order (After Go-Live)	T+2.25
3.	Floating tender for Aadhaar HW and SW	T+0.5
4.	Tender evaluation	T+1.5
5.	Award of Contract	T1=T+2.0
6.	Supply & installation of hardware	T1 +1.5
7.	Customization & deployment of software	T1 + 2
8.	UAT & training	T1 + 2.5
9.	Rollout/Go Live	T1 + 3
10.	Warranty	T1 + 60

*****