Megha Engineering & Infrastructures Ltd

An ISO 9001-2008 Company

#10,1st Floor, 3rd Main, 16th Cross, G.D Park Extension, Vyalikaval, Bangalore-560003

Tel: +91-80-23311722, Fax: +91-80-23311723 Email:blrro@meilgroup.com

CIN No.:U15202AP2006PLC050271

MEIL/ BWSSB-CP-04/2021-22/061 **Date: 16.07.2021**

To

Executive Engineer,
EE(CH) Division,
BWSSB, TK Halli,
Karnataka - 571421.

Sub: Design/Engineering, Construction, Commissioning of Pump Station and Reservoir at Harohalli and Tataguni with Operations and Maintenance of Seven (7) Years– **"Regarding the submission of Compliance for providing Management Information System (MIS) Specification and Scope -CP-04 Project"**

Ref: 1. Agreement no.: BWSSB –III/CP-04/05/2020-21Dt: 04.09.2020.
2. LOA: BWSSB/CEKTE/TA11/37/2020/1560/2020-21 Dt: 05.08.2020.
3. Your Lr.no. BWSSB/EECH/CH-2/CP-04/42/2020-21 Dt: 21.05.2021.

Sir,

Adverting to the above reference 3rd cited, we hereby submitting our compliance for providing Management information system (MIS) software.

It is to inform you that, we have placed the order to the approved vendor of BWSSB - M/s. Exto Project Solution Private Ltd. for providing the MIS Software as required by the client. As the MIS Software requirement details are not briefly explained in the agreement, so we have developed some Dash board based available details in the agreement.

We request your good offices to deploy some representative to work with Exto team, since the Software is customized and to be developed as per the BWSSB requirement.

We hope, As the M/s. Exto Project Solution Pvt. Ltd. is recommended by Client, the documents like SLA details, Cloud server documents, data encryption documents etc., has been already collected and verified earlier itself before given approval of vendor. Even though we have enclosed the documents as provided by Exto.

Yours faithfully,
For **Megha Engineering & Infrastructures Limited**

(Authorized Signatory)
Encl: As above

1. **The Chief Engineer, 5th Floor, Cauvery Bhavan, Bangalore:** For your kind information.
2. **The Additional Chief Engineer, ACE(K), Cauvery Bhavan, 5th floor, Bangalore:** For your kind information.
3. **ONTB, Team Leader:** For your kind information and further needful.

BWSSP (PHASE-3), STAGE - V	
Date Recd.	20/07/2021
Chrono In No.	ONTB-5440
File Name	CP-04
File No.	02
Copies To	Queen ★ with Enclosures
Circulate to & Then to File	
Action By	
Reply Chrono	
Out No.	
Reply Date	

meil

Compliance for the Comments made by BWSSB Lr.no.: BWSSB/EECH/CH-2/CP-04/42/2020-21 Dt: 21.05.2021

Sl.No	Comments from ONTB	Reply from MEIL
1	The contractor shall include a complete specification as per requirements of the contract. The submitted document is not matching the contract requirements and is deviation from the contract requirements. Contractor shall revise to include the complete scope as per contract requirements.	As per the Agreement clause no. 3.6 of Management Information System (MIS), the mentioned specifications are included in submitted documents. The complete specifications mentioned are given below, 1). Design Progress. 2). Daily Progress on site. 3). Physical Progress of the project. 4). Financial Progress of the project. 5). Issues and Hindrances. 6). Forecasting reports. 7). Estimated time of completion etc., 8). Document attachments/upload (Document management system). 9). Charts and graphs to depict the above, inclusive of reports. 10). Tracking the above via Android app on Mobile phones. 11). Document submission status tracking. 12). CCTV real time feed from the site locations. **Agreement copy is enclosed as Annexure-A.**
2	The contractor shall include the following: Measurement book Project scheduler RA Bills Online live CCTV feeds in real time. 5 number of concurrent users ID for each work site. Separate MIS shall be used for individual projects.	1) Measurement book - Noted and it will come under financial Progress of the Project. 2). Project scheduler - Noted and it will be included. 3). RA Bills - Noted and it will come under Financial Progress of the Project. 4). Online live CCTV feeds in real time - Online live CCTV feeds link will be provided in Dashboard. 5). 5 number of concurrent users ID for each work site - Noted and As already mentioned minimum 2 to 5 users will be provided for each project. **(enclosed as Annexure-B)**. 6). Separate MIS shall be used for individual projects - Noted.
3	The contractor shall include the complete document management system. Submit complete features of the system. Contractor shall note that there shall be a separate document management system for each work site. Revise to include the same.	We have Provided complete document management system as mentioned in the agreement. If anything to be added, it can be added while configuring at your office. As the document submitted to you was the demo/initial documents, and the software is customised for as per BWSSB requirements, any addition / modification can be done while configuring at your office on day to day basis. We confirm that Project wise document management system will be provided as we are providing project wise software license.
4	The SLA agreement shall be with 99.99% .The same shall be submitted for review and approval. The current SLA agreement indicated is not acceptable. Revise to include as per contract requirements.	SLA agreement copy is enclosed as **Annexure-C.**
5	The document submitted indicates only 3 numbers of reports. Why is there a limitation on the number of reports and users for the system? This shall be unlimited. Revise to include the same.	Noted. Kindly provide the details for what are the items, the reports need to be provided to mention in Dash board. The No of users will be provided as mentioned above.
6	The contract requires a minimum 10 TB is cloud space. However the contractor has included only 100 GB of space. Revise to include the same and submit documentation as confirmation.	10TB cloud space has not mentioned in the agreement. Initially we have provided the space of 100GB. We (MEIL) undertake that any addition of space will be provided whenever required.
7	The contractor shall include integration with the BWSSB MIS system, which is currently not included by the contractor. Revise to include the same.	We confirm that we will provide the data and necessary support for the integration with the BWSSB MIS system. For that, kindly provide the details of modules and the requirements of BWSSB MIS system for integration.
8	The contractor shall submit details of that cloud server and where it is being hosted. Data encryption policy shall be submitted.	EXTO Application and DB Servers are hosted in the Microsoft Azure cloud located in central India and running on Cent OS. Data encryption policy is enclosed as **Annexure-D.**
9	Contractor shall submit data encryption certificate for review and approval.	We have provided a VAPT certificate of "EXTO PROJECT SOLUTIONS PRIVATE LIMITED" for the Data encryption with vulnerability and penetration test. The same has enclosed as **Annexure-E.** If any other certifcate required, kindly provide the details to arrange.
10	The contractor has indicated that the system ownership shall be retained by the vendor and not by BWSSB. This is not as per contract requirements. Revise to include ownership of the software and data by BWSSB.	The ownership of the software will be in MEIL only. As per the agreement we have to provide and impletmentation of Management information system till the project completion and handing over the scheme to the client.
11	Contractor shall submit comment resolution sheet and highlight the revisions with a revision cloud for easy cross referencing and review.	Noted.

Annexure-A

and stop equipment, provide configuration tools and operate diagnostic facilities from Operator Workstations (OW) and Engineers workstation (EW), after successful log-on by security password.

The System shall perform all the necessary functions for the optimum monitoring, automatic control and operation of the entire system. The SCADA control room shall be equipped with false flooring to provide access for all cables. No cables shall be installed over the control room floor.

7.9 Management Information System:

The contractor under this contract shall be responsible for provision and implementation of Management improvement system which shall be inclusive of required software, hardware, high speed internet bandwidth, required programming to have integration and complete project monitoring of the project remotely from Cauvery Bhavan by BWSSB and project management consultants. The MIS system shall provide a digital platform for monitoring the project remotely. The contractor MIS software shall be integrated in real time with the BWSSB MIS software.

The MIS system shall enable real time project status monitoring and shall provide a real time project dashboard to BWSSB and project management consultants.

On a minimum, the following shall from an essential part of the MIS system but not limited to:

Design progress
Daily progress on site
Physical progress of the project
Financial progress of the project
Issues & Hindrances
Forecasting reports
Estimated Time of completion etc.
Document attachments/upload (Code-B & Code-A ,All project documentation)(Document management system)
Charts and graphs to depict the above, inclusive of reports
Document submission status tracking
Tracking the above via Android app on Mobile phones
CCTV real time feed from the site locations

The contractor shall implement and maintain the system right from the start of the project till the end of the project and handing over.

End of Part-7

Annexure-B

Scope and specifications:

EXTO For Individual package MIS - Respective Packages

Every Contractor / JV is expected to subscribe to Exto monitoring services to monitor their respective packages. Expected benefits,

1. One source of truth for all Project communication across all Project stake holders
2. Pre configured reports / Dashboards and the reporting mechanism between the Contractors and PMC's reduce well defined in the system and the Contractors / JV's will be trained to use the system most effectively
3. System to ensure smooth data flow, Approval workflows and document control – Expected to minimize time lost due to mismatch of formats.
4. Since Reports and Dashboards and the monitoring mechanisms are configured to ensure the contractor/ JV could use it for their internal reporting, this eliminates the duplication efforts in terms of preparation /submission of monitoring reports on routine
5. Being a highly Interactive platform, this could be used to highlight issues and hindrances faced by Contractors to Project stake holders which is expected to provide better visibility on the issues and the respective status
6. Appropriate notifications and other control mechanisms in the system would provide clear visibility on the Project status, visibility on the status of approvals / delays which helps to streamline timely actions.
7. Since both PMC and Contractor are expected to be in the same system, there are high possibilities that the wok progress/ measurement and the certification could be effectively tracked which would be supportive for the contractors to reduce the billing cycle time.
8. Since all Project documents / communications are in the system, it would be helpful to trace back in case claims process.

Scope:

The system is to be used for the MEIL Package CP-04 of BWSSB Cauvery stage 5 project only.

Scope of the project includes only following modules,

The complete specifications mentioned are given below,

- Design Progress.
- Daily Progress on site.
- Physical Progress of the project.
- Financial Progress of the project.
- Issues and Hindrances.
- Forecasting reports.
- Estimated time of completion etc.,
- Document attachments/upload (Document management system).
- Charts and graphs to depict the above, inclusive of reports.
- Tracking the above via Android app on Mobile phones.
- Document submission status tracking.
- CCTV real time feed from the site locations.
- The System is provisioned for Minimum 2 to 5 years.

Annexure-C

exto

Exto Service level Agreement

Exto is hosted on Intel's Microsoft Azure IaaS and as such is designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth.

Microsoft guarantees that Apps running in a customer subscription will be available 99.5% of the time within its public Azure cloud. Commencing at the activation of your production Exto environment post implementation, Exto will work with Intel to meet the Target Service Availability Level, or Target Service Uptime, of 99.5% for Exto within Azure environment subject to Azure cloud environment, maintenance and uptime metrics.

The SLA does not apply to any (a) features designated pre-general availability (b) alpha/beta features excluded from the SLA or (c) errors (i) caused by factors outside of Exto's reasonable control; (ii) that resulted from Customer's software or hardware or third party software or hardware, or both; (iii) that resulted from abuses or other behaviours that violate the Agreement; (iv) Service disruption due to Force Majeure, including, but not limited to, natural disasters, war or acts of terrorism, or government's actions.

Annexure - D

Table of Contents

Azure Data Encryption policy

Azure Storage encryption for data at rest

Azure Storage uses server-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.

About Azure Storage encryption

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

Azure Storage encryption is enabled for all storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications to take advantage of Azure Storage encryption.

Data in a storage account is encrypted regardless of performance tier (standard or premium), access tier (hot or cool), or deployment model (Azure Resource Manager or classic). All blobs in the archive tier are also encrypted. All Azure Storage redundancy options support encryption, and all data in both the primary and secondary regions is encrypted when geo-replication is enabled. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. There is no additional cost for Azure Storage encryption.

Every block blob, append blob, or page blob that was written to Azure Storage after October 20, 2017 is encrypted. Blobs created prior to this date continue to be encrypted by a background process. To force the encryption of a blob that was created before October 20, 2017, you can rewrite the blob.

About encryption key management

Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to manage encryption with your own keys, you have two options. You can use either type of key management, or both:

- You can specify a *customer-managed key* to use for encrypting and decrypting data in Blob storage and in Azure Files.[1,2] Customer-managed keys must be stored in Azure Key Vault or Azure Key Vault Managed Hardware Security Model (HSM)

- You can specify a *customer-provided key* on Blob storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted

The following table compares key management options for Azure Storage encryption.

ABOUT ENCRYPTION KEY MANAGEMENT			
Key management parameter	**Microsoft-managed keys**	**Customer-managed keys**	**Customer-provided keys**
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob storage, Azure Files[1,2]	Blob storage
Key storage	Microsoft key store	Azure Key Vault or Key Vault HSM	Customer's own key store
Key rotation responsibility	Microsoft	Customer	Customer
Key control	Microsoft	Customer	Customer

Doubly encrypt data with infrastructure encryption

Customers who require high levels of assurance that their data is secure can also enable 256-bit AES encryption at the Azure Storage infrastructure level. When infrastructure encryption is enabled, data in a storage account is encrypted twice — once at the service level and once at the infrastructure level — with two different encryption algorithms and two different keys. Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. In this scenario, the additional layer of encryption continues to protect your data.

Service-level encryption supports the use of either Microsoft-managed keys or customer-managed keys with Azure Key Vault. Infrastructure-level encryption relies on Microsoft-managed keys and always uses a separate key.

Azure Data Encryption at rest

Microsoft Azure includes tools to safeguard data according to your company's security and compliance needs. This paper focuses on:

- How data is protected at rest across Microsoft Azure

- Discusses the various components taking part in the data protection implementation,
- Reviews pros and cons of the different key management protection approaches.

Encryption at Rest is a common security requirement. In Azure, organizations can encrypt data at rest without the risk or cost of a custom key management solution. Organizations have the option of letting Azure completely manage Encryption at Rest. Additionally, organizations have various options to closely manage encryption or encryption keys.

Encryption is the secure encoding of data used to protect confidentiality of data. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model:

- A symmetric encryption key is used to encrypt data as it is written to storage.
- The same encryption key is used to decrypt that data as it is readied for use in memory.
- Data may be partitioned, and different keys may be used for each partition.
- Keys must be stored in a secure location with identity-based access control and audit policies. Data encryption keys are often encrypted with a key encryption key in Azure Key Vault to further limit access.

In practice, key management and control scenarios, as well as scale and availability assurances, require additional constructs. Microsoft Azure Encryption at Rest concepts and components are described below.

The purpose of encryption at rest

Encryption at rest provides data protection for stored data (at rest). Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. In such an attack, a server's hard drive may have been mishandled during maintenance allowing an attacker to remove the hard drive. Later the attacker would put the hard drive into a computer under their control to attempt to access the data.

Encryption at rest is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. If an attacker obtains a hard drive with encrypted data but not the encryption keys, the attacker must defeat the encryption to read the data. This attack is much more complex and resource consuming than accessing unencrypted data on a hard drive. For this reason, encryption at rest is highly recommended and is a high priority requirement for many organizations.

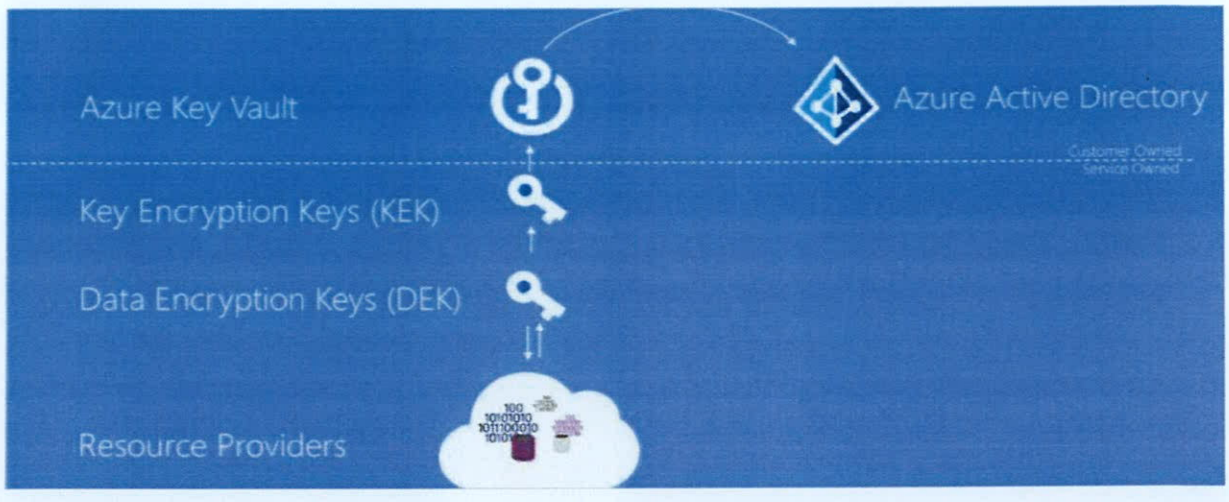
Encryption at rest may also be required by an organization's need for data governance and compliance efforts. Industry and government regulations such as HIPAA, PCI and FedRAMP, lay out specific safeguards regarding data protection and encryption requirements. Encryption at rest is a mandatory measure required for compliance with some of those regulations.

In addition to satisfying compliance and regulatory requirements, encryption at rest provides defense-in-depth protection. Microsoft Azure provides a compliant platform for services, applications, and data. It also provides comprehensive facility and physical security, data access control, and auditing. However, it's important to provide additional "overlapping" security measures in case one of the other security measures fails and encryption at rest provides such a security measure.

Microsoft is committed to encryption at rest options across cloud services and giving customers control of encryption keys and logs of key use. Additionally, Microsoft is working towards encrypting all customer data at rest by default.

Azure Encryption at Rest Components

As described previously, the goal of encryption at rest is that data that is persisted on disk is encrypted with a secret encryption key. To achieve that goal secure key creation, storage, access control, and management of the encryption keys must be provided. Though details may vary, Azure services Encryption at Rest implementations can be described in terms illustrated in the following diagram.



Azure Key Vault

The storage location of the encryption keys and access control to those keys is central to an encryption at rest model. The keys need to be highly secured but manageable by specified users and available to specific services. For Azure services, Azure Key Vault is the recommended key storage solution and provides a common management experience across services. Keys are stored and managed in key vaults,

and access to a key vault can be given to users or services. Azure Key Vault supports customer creation of keys or import of customer keys for use in customer-managed encryption key scenarios.

Azure Active Directory

Permissions to use the keys stored in Azure Key Vault, either to manage or to access them for Encryption at Rest encryption and decryption, can be given to Azure Active Directory accounts.

Key Hierarchy

More than one encryption key is used in an encryption at rest implementation. Storing an encryption key in Azure Key Vault ensures secure key access and central management of keys. However, service local access to encryption keys is more efficient for bulk encryption and decryption than interacting with Key Vault for every data operation, allowing for stronger encryption and better performance. Limiting the use of a single encryption key decreases the risk that the key will be compromised and the cost of re-encryption when a key must be replaced. Azure encryptions at rest models use a key hierarchy made up of the following types of keys in order to address all these needs:

- Data Encryption Key (DEK) – A symmetric AES256 key used to encrypt a partition or block of data. A single resource may have many partitions and many Data Encryption Keys. Encrypting each block of data with a different key makes crypto analysis attacks more difficult. Access to DEKs is needed by the resource provider or application instance that is encrypting and decrypting a specific block. When a DEK is replaced with a new key only the data in its associated block must be re-encrypted with the new key.
- Key Encryption Key (KEK) – An encryption key used to encrypt the Data Encryption Keys. Use of a Key Encryption Key that never leaves Key Vault allows the data encryption keys themselves to be encrypted and controlled. The entity that has access to the KEK may be different than the entity that requires the DEK. An entity may broker access to the DEK to limit the access of each DEK to a specific partition. Since the KEK is required to decrypt the DEKs, the KEK is effectively a single point by which DEKs can be effectively deleted by deletion of the KEK.

The Data Encryption Keys, encrypted with the Key Encryption Keys are stored separately and only an entity with access to the Key Encryption Key can decrypt these Data Encryption Keys. Different models of key storage are supported

Encryption at rest in Microsoft cloud services

Microsoft Cloud services are used in all three cloud models: IaaS, PaaS, SaaS. Below you have examples of how they fit on each model:

- Software services, referred to as Software as a Server or SaaS, which have applications provided by the cloud such as Microsoft 365.
- Platform services which customers leverage the cloud in their applications, using the cloud for things like storage, analytics, and service bus functionality.
- Infrastructure services, or Infrastructure as a Service (IaaS) in which customer deploys operating systems and applications that are hosted in the cloud and possibly leveraging other cloud services.

Encryption at rest for SaaS customers

Software as a Service (SaaS) customers typically have encryption at rest enabled or available in each service. Microsoft 365 has several options for customers to verify or enable encryption at rest.

Encryption at rest for PaaS customers

Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine.

Encryption at rest for IaaS customers

Infrastructure as a Service (IaaS) customers can have a variety of services and applications in use. IaaS services can enable encryption at rest in their Azure hosted virtual machines and VHDs using Azure Disk Encryption.

Encrypted storage

Like PaaS, IaaS solutions can leverage other Azure services that store data encrypted at rest. In these cases, you can enable the Encryption at Rest support as provided by each consumed Azure service. The Data encryption models: supporting services enumerates the major storage, services, and application platforms and the model of Encryption at Rest supported.

Encrypted compute

All Managed Disks, Snapshots, and Images are encrypted using Storage Service Encryption using a service-managed key. A more complete Encryption at Rest solution ensures that the data is never persisted in unencrypted form. While processing the data on a virtual machine, data can be persisted to the Windows page file or Linux swap file, a crash dump, or to an application log. To ensure this data is encrypted at rest, IaaS applications can use Azure Disk Encryption on an Azure IaaS virtual machine (Windows or Linux) and virtual disk.

Custom encryption at rest

It is recommended that whenever possible, IaaS applications leverage Azure Disk Encryption and Encryption at Rest options provided by any consumed Azure services. In some cases, such as irregular encryption requirements or non-Azure based storage, a developer of an IaaS application may need to implement encryption at rest themselves. Developers of IaaS solutions can better integrate with Azure management and customer expectations by leveraging certain Azure components. Specifically, developers should use the Azure Key Vault service to provide secure key storage as well as provide their customers with consistent key management options with that of most Azure platform services. Additionally, custom solutions should use Azure-Managed Service Identities to enable service accounts to access encryption keys. For developer information on Azure Key Vault and Managed Service Identities, see their respective SDKs.

Azure resource providers encryption model support

Microsoft Azure Services each support one or more of the encryption at rest models. For some services, however, one or more of the encryption models may not be applicable. For services that support customer-managed key scenarios, they may support only a subset of the key types that Azure Key Vault supports for key encryption keys. Additionally, services may release support for these scenarios and key types at different schedules. This section describes the encryption at rest support at the time of this writing for each of the major Azure data storage services.

Azure disk encryption

Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption.

Azure storage

All Azure Storage services (Blob storage, Queue storage, Table storage, and Azure Files) support server-side encryption at rest; some services additionally support customer-managed keys and client-side encryption.

- Server-side: All Azure Storage Services enable server-side encryption by default using service-managed keys, which is transparent to the application. Azure Blob storage and Azure Files also support RSA 2048-bit customer-managed keys in Azure Key Vault.
- Client-side: Azure Blobs, Tables, and Queues support client-side encryption. When using client-side encryption, customers encrypt the data and upload the data as an encrypted blob. Key management is done by the customer

Azure SQL Database:

Azure SQL Database currently supports encryption at rest for Microsoft-managed service side and client-side encryption scenarios.

Support for server encryption is currently provided through the SQL feature called Transparent Data Encryption. Once an Azure SQL Database customer enables TDE key are automatically created and managed for them. Encryption at rest can be enabled at the database and server levels. As of June 2017, Transparent Data Encryption (TDE) is enabled by default on newly created databases. Azure SQL Database supports RSA 2048-bit customer-managed keys in Azure Key Vault.

Client-side encryption of Azure SQL Database data is supported through the Always Encrypted feature. Always Encrypted uses a key that created and stored by the client. Customers can store the master key in a Windows certificate store, Azure Key Vault, or a local Hardware Security Module. Using SQL Server Management Studio, SQL users choose what key they'd like to use to encrypt which column.

Conclusion

Protection of customer data stored within Azure Services is of paramount importance to Microsoft. All Azure hosted services are committed to providing Encryption at Rest options. Azure services support either service-managed keys, customer-managed keys, or client-side encryption. Azure services are broadly enhancing Encryption at Rest availability and new options are planned for preview and general availability in the upcoming months.

Annexure - E

CERTIFICATE

Of Compliance

This Certificate of Compliance is here by issued to the below named company.

EXTO PROJECT SOLUTIONS PRIVATE LIMITED

3, Sankarpuram, Aalamelumangapuram, Mylapore, Chennai, Tamilnadu- 600004

The organization's Web Application **EXTO360** has been found in compliance with global Vulnerability Assessment & PenetrationTesting guidelines

Certificate number: 1600446

08-Jan-2021

Date

MG Vinay Kumar
Director

Veave

www.veave.in
contact@veave.in