White Paper

How Noah Mobile uses Microsoft Azure Core Services

The Noah Mobile Cloud service is built for the Microsoft Azure platform. The solutions that are part of the Noah Mobile cloud service are based on the core Platform-as-a-Service (PaaS) services on the Microsoft Azure Platform.

The Noah Mobile Cloud Service use a subset of the core PasS services that are an integrated part of the Azure platform.

The Noah Mobile Cloud Service use the following Microsoft Core Services:

- Azure Servicebus
- Azure Storage
    - Azure Table Storage
    - Azure Blob Storage
- Azure SQL Server (For HIMSA internal configuration data)
- Azure Traffic Manager

All Microsoft Azure services that are used as a part of the Noah Mobile Cloud Service are independently verified and:

- ISO 27001 certified
- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- HIPAA BAA compliant
- DPA/EU-model clause compliant
- FISMA and FedRAMP

Azure Services used by Noah Mobile Cloud

The following section describe the Azure Core Services used by the Noah Mobile Cloud Service.

Azure Servicebus

Service Bus Relay solves the challenges of communicating between on-premises applications and the outside world by allowing on-premises web services to project public endpoints.

The Service Bus Relay is designed for the use-case of taking existing Windows Communication Foundation (WCF) web services and making those services securely accessible to solutions that reside outside the corporate perimeter without requiring intrusive changes to the corporate network infrastructure. Such Service Bus Relay services are still hosted inside their existing environment, but they delegate listening for incoming sessions and requests to the cloud-hosted Service Bus. The Service Bus also protects those services from unauthorized access by using Azure Active Directory Access Control.

Azure Storage

The Noah Mobile Cloud Service uses Microsoft Azure Storage for storing data used by the cloud service. The cloud service only stores data for the cloud service, and no patient data or other local data from the Noah Server is stored by the cloud service.

Microsoft Azure Storage is built on a “log-based file system”, meaning anytime that anything is written to Azure Storage (whether in a blob or table entity), it never overwrites an existing value on a disk. Instead, all writes (regardless of what object is being written) are written into a circular queue which is flushed to physical disks. This provides extra assurance against corruption as no transaction is ever finalized until the new data is in place.

Azure Storage nodes are all independent from Azure Compute machines. They are deployed on separate hardware, each with its own management and security model. Specifically, Azure Storage executes access control policies, and all storage requests must be authenticated. Authentication relies on a Bearer Token model. Access to the data stored in the Azure table or blob storage requires that the client possess the correct token (key) before they are granted access to the data.

Azure SQL Server

The Noah Mobile Cloud Service uses Azure SQL database for storing user profiles for accessing the Noah Mobile administration module. The only users that can administer Noah Mobile Cloud Services (setting up new apps or looking at statistics per app) are HIMSA employees. It does not give the HIMSA employee access to any local Noah data presiding on a remote host, and does not give any access to keys or other data related to the security or access to data.

Azure SQL Database is a PaaS relational database offering. Customers are granted access to their databases through standard interfaces while administration of the underlying system is managed by the Azure platform and Microsoft.

Azure SQL Database, while very similar to SQL Server, has different design goals which result in functional differences when compared to SQL Server running in an on-premise environment.

Microsoft provides configuration, upgrades, and patching of the Azure SQL Database platform.

Azure SQL Database is a PaaS relational database offering. Customers are granted access to their databases through standard interfaces while administration of the underlying system is managed by the Azure platform and Microsoft.

Azure Traffic Manager

The Noah Mobile Cloud Service production environment uses the Azure Traffic Manager Service to control the distribution of user traffic.

Traffic Manager is used for:

- Improved availability – Traffic Manager allows us to improve the availability of the Noah Mobile Cloud Service by monitoring the service endpoints in Azure and providing automatic failover capabilities.
- Improved responsiveness for the service – Azure allows us to run cloud services in datacenters located around the world. Traffic Manager can improve the responsiveness of the service and content delivery times by directing end-users to the endpoint with the lowest network latency from the client.

Security Controls and Capabilities

Microsoft Azure delivers a trusted foundation on which the Noah Mobile cloud service is designed.

Azure provides a cloud environment with integrated security controls and capabilities designed for secure operations:

- **24/7/365 Monitored physical security**
  Data centers are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

- **Monitoring and logging**
  Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

- **Patching**
  Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.

- **Antivirus/Antimalware protection**
  Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.

- **Intrusion detection and DDoS**
  Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.

- **Zero standing privileges**
  Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.

- **Isolation**
  Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.

- **Encrypted communications**
  Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises data centers, and from Azure to administrators and users.

- **Data encryption**
  Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meet their needs.

Compliance

To address the wide range of international, country, and industry-specific regulatory requirements the Microsoft Azure platform is independently verified.

Microsoft provides Azure customers with detailed information about the security and compliance programs for the Microsoft Azure Platform, including audit reports and compliance packages.

ISO 27001:2005 Audit and Certification

The Microsoft Azure platform goes through an annual certification process against the ISO/IEC 27001:2005 security standard.

The ISO 27001:2005 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. The certificate issued by the British Standards Institution (BSI) is publically available.

SOC 1 and SOC 2 SSAE 16/ISAE 3402 Attestations

Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements.

The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).

Cloud Security Alliance Cloud Controls Matrix

Azure has been audited against the Cloud Controls Matrix (CCM) established by the Cloud Security Alliance (CSA). The audit was completed as part of the SOC 2 Type 2 assessment, the details of which are included in that report. This combined approach is recommended by the American Institute of Certified Public Accountants (AICPA) and CSA as a means of meeting the assurance and reporting needs of the majority of cloud services users.

The CSA CCM is designed to provide fundamental security principles to guide cloud vendors and to assist prospective customers in assessing the overall security risk of a cloud provider. By having completed an assessment against the CCM, Azure offers transparency into how its security controls are designed and managed with verification by an expert, independent audit firm.

Detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM is also published in the CSA's Security Trust and Assurance Registry (STAR).

Platform Encryption

Among Microsoft Azure’s data protection capabilities are built-in services, components and configurations that apply encryption to internal data and traffic. These serve to enable enhanced security for customer information, and also help enforce data governance and compliance with industry regulations (and are mandated as such).

Azure implements encryption using both symmetric and asymmetric keys for encrypting and protecting confidentiality of data:

- Software-based AES-256 for symmetric encryption/decryption
- 2048-bit or better for asymmetric keys
- SHA-256 or better for secure hashing

Security Processes

Shared Responsibility Environment

Because the Noah Mobil Cloud Service is based on the Microsoft Azure platform infrastructure it creates a shared responsibility model between the Himsa as the provider of the Noah Cloud Service and Microsoft.

This shared model reduce the operational burden as Microsoft operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

The Noah customer has the responsibility of adhering to the legal requirements and security controls needed when operating the Noah Server, this falls outside Himsa’s scope of control.

Infrastructure Security

Microsoft operates the cloud infrastructure that is used to provision a variety of basic computing resources such as processing and storage.

The Azure infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The Microsoft Azure infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards.

Physical and Environmental Security

Microsoft's data centers are state of the art, utilizing innovative architectural and engineering approaches. Microsoft has many years of experience in designing, constructing, and operating large scale data centers. This experience has been applied to the Microsoft Azure platform and infrastructure.

Microsoft data centers are housed in nondescript facilities and the physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week.

Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility.

The Azure data centers use generators to provide backup power for the entire facility.