# Technical Design Document

## Onix Platform

## Contents

# 1. Introduction

## 1.1. Purpose

This document outlines the technical architecture, components, services, and security measures implemented in the Onix solution. It serves as a reference for development, deployment, and maintenance phases

## 1.2. Scope

The document covers the Onix platform, including all Onix applications and services.

It details the application hosting, data storage, security, and backup strategies.

## 1.3 Audience

This document is intended for developers, IT professionals, and system administrators involved in the implementation and operation of Onix infrastructure and applications.

# 2. System Architecture Overview

Onix is a SaaS solution, with optional installation of features and client apps on-premises.

The solution architecture is built on Microsoft Azure, leveraging both IaaS and PaaS models to offer scalable, reliable, and secure applications. It includes Azure Virtual Servers, Azure App Services, Azure SQL Managed Servers, Azure Block Blob Storages, Azure File Shares, and various other Azure services for optimal performance and resilience.

Below is a high-level service diagram that illustrates the Azure Cloud Service Model employed for Microsoft Azure.

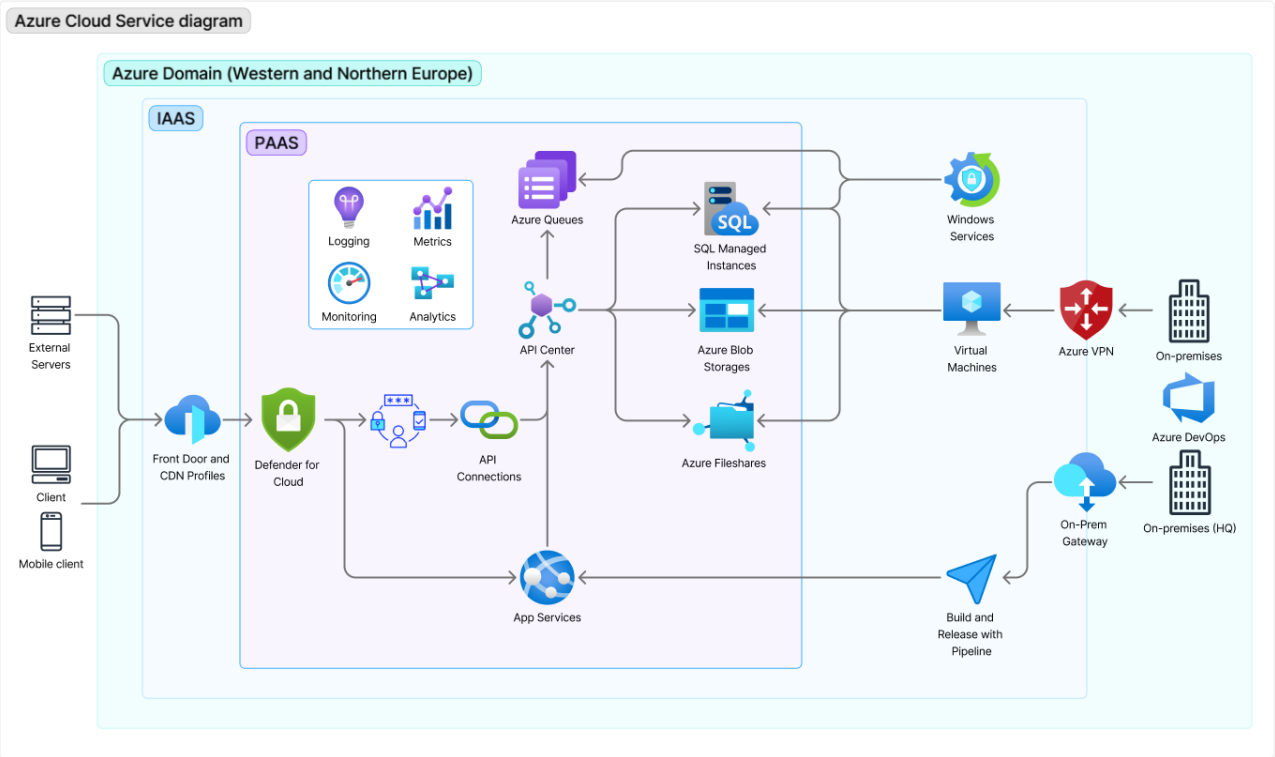


*Figure 1: Azure Cloud Service Diagram for Onix*

# 3. Architecture Components

## 3.1. Azure Platform as a Service (PaaS) Model

Onix's applications are hosted using Azure App Service. This is PaaS offering that enables building, deploying, and scaling enterprise-grade web apps with ease.

## 3.2. Azure Infrastructure as a Service (IaaS) Model

The IaaS model includes services hosted on Azure Virtual Machines, such as IIS for web applications and Windows services, which are essential for certain background processes and tasks.

## 3.3. Storage Solutions

- Azure SQL Managed Instance is used for relational database needs
- Azure Blob Storage for unstructured data storage
- Azure File Share to manage internally shared files across services
- Azure Queue is an integral part of the system, managing communication between different components via message queuing.

## 3.4. External APIs and Hybrid Connectivity

The system is designed to interact seamlessly with external APIs and supports access from various client devices, including Windows, mobile applications, and browsers. It also maintains connectivity with on-premises servers for a comprehensive hybrid cloud strategy.

## 3.5. Hosted Environments

Onix hosts 4 environments

- Production
- Sandbox
- Test
- Development

The environments are technically identical, but data is encrypted for Test and Development.

The Sandbox environment contains data identical to production, but with a latency of up to 8 weeks

# 4. Data Protection and Security

## 4.1 Data protection

All keys and certificates are protected by Azure Key Vault, and can only be accessed by named managers.

Data At Rest is protected with Transparent Data Encryption (TDE) and AES-256 encryption.

## 4.2 Security

The security of our cloud infrastructure is bolstered by Microsoft Defender for Cloud, providing advanced threat protection and security management.

Data In Transit is secured with Transport Layer Security 1.2 (TLS 1.2 / SHA-256).

### 4.3 Authentication

Information in Onix is protected by user authentication.

Main object for identification is email-address.

Both internal identity provider and Azure identity provider is supported.

Azure Identity provider:

- SSO/MFA will be available through Azure Identity provider.
- OAuth 2.0/OIDC based authentication.
- Open API is secured by API Key or bearer.

Onix Identity provider:

- OAuth 2.0/OIDC based authentication.
- Password format: minimum 8 characters containing number(s) and LC/UC letter(s).
- Passwords are stored and handled encrypted and cannot under any circumstances be reversed.
- Passwords are self-handled, and will not expire by any given frequency.

### 4.4 Authorization

Role based authorization is handled inside Onix.

RBAC/Group Claims are supported for Azure identity provider.

### 4.5 Security Measures

Regular security assessments and updates are conducted to ensure the infrastructure and applications are protected against known vulnerabilities.

An independent third-party security firm performs an annual penetration test against all externally and internally accessible endpoints.

## 5. Backup and recovery

The solution is designed with a robust disaster recovery plan, utilizing Azure's geo-redundant storage and backup capabilities to ensure business continuity.

Onix is a B2B system, were all data remains in the same storage. As for B2B system in general, data recovery is solely for disaster recovery purposes.

### 5.1 Recover Point Objective (RPO)

Close to no data loss.

Onix has an instant backup function, meaning that all data are transferred immediately to separate backup sources during save-operations.

Only data in transfer and unfinished transactions will be lost in case of system failure.

### 5.2 Recovery Time Objective (RTO)

Less than 3 days.

Depending on the source of system failure, the structures and data can be reconstructed in less than 3 days. Onix depends on the availability of Azure located in Northern and Western Europe.

## 6. Development Environment

The development environment is configured to mirror production settings as closely as possible, ensuring reliability of testing.

All developers have been trained in security and follows internal procedures and guidelines to ensure that our strong requirements are followed up in any layer of our system.

### 6.1 Tools for development and quality assurance

Developer's main tool is Microsoft Visual Studio.

All source code is handled by Azure DevOps.

### 6.2 Source Control and CI/CD Pipeline

Source code management is facilitated through a version control system. Continuous Integration and Continuous Deployment (CI/CD) are automated through Azure Pipelines, allowing for efficient, reliable, and consistent updates to production environments.

### 6.3 Open Source libraries

The software uses exclusively open source libraries with one of the following license agreements:

| | |
|---|---|
| Apache-2.0 | https://www.apache.org/licenses/LICENSE-2.0.txt |
| BSD-2-Clause/ BSD-3-Clause | https://opensource.org/license/bsd-3-clause |
| MIT | https://opensource.org/license/mit |

## 7. Monitoring and Logging

System health, performance metrics, and operational logs are managed using Azure Monitoring and Logging services, ensuring that we have real-time insights into our system's performance.

Logs can be made available for customers on request.

Most entries for create and update operations are visible by the object inside Onix applications. Logs for delete can be obtained on request.

## 8. Incident Reporting

Incidents are handled by priority based on criticality.

Documentation of incidents: Internal QHSE documents, Salesforce, Azure DevOps.

## 9. Service Level (SL)

99,79% expected uptime including maintenance windows, 99.99% without.

Onix solely makes use of services in Azure that in average has an uptime greater than 99,99%.

### 9.1. Maintaining windows

Onix performs monthly maintenance, and bi-monthly releases (in average).

The maintenance window is announced, and the system will remain unresponsive for periods within these windows.

### 9.2. Technical support

Onix has an online technical support, open 24/7 and manned minimum 12 hrs./day weekdays.

Downtime is automatically reported through monitoring, and alerts are supervised 24/7.

## 10. Compliance

The system is designed to comply with relevant data protection and privacy laws, employing best practices in data handling and security.

## 11. Conclusion

Onix provides a secure, scalable, and resilient solution for business operations, underpinned by a sophisticated Azure Cloud Service Model. This Technical Design Document outlines the strategic approach to our cloud-based infrastructure, ensuring optimal performance and security.