xytech
www.xytechsystems.com

MediaPulse Managed Cloud Revealed

Xytech Systems Corporation
www.XytechSystems.com + 818-698-4900 +44 20-3478-1450

RELEASED APRIL 16, 2019

Xytech Systems Corporation • 9410 Topanga Canyon Blvd., Suite 200
Chatsworth, CA, USA 91311

Xytech Systems UK Ltd. • 28 Margaret Street, 3rd floor • London W1W 8RZ UK

www.xytechsytems.com

xytech
www.xytechsystems.com

Contents

INTRODUCTION

Xytech uses Microsoft's Azure Cloud as a platform for its MediaPulse Facility Management System. Using Sky, a browser-based User Interface, you can manage your facility and control your assets from anywhere, using any popular device, including PC, Mac, Tablet and Smartphone.

The availability and security of your information is a primary concern to both you and us. Xytech takes advantage of the built-in resiliency and redundancy offered by the Azure Cloud along with their cloud security services. These are layered on top of our own security mechanisms.

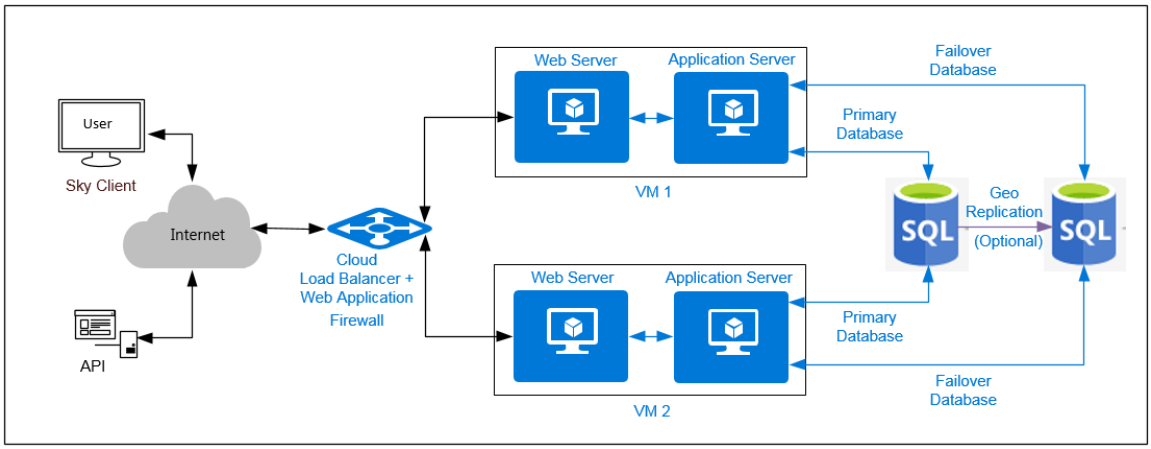
Microsoft's Azure Cloud has ubiquitous connectivity and near-100% availability, making it the ideal platform to run mission-critical applications like MediaPulse. Xytech's Azure cloud is maintained by Azure certified experts.

Finding a Home in the Cloud

Entering the Cloud

Connection to MediaPulse starts at a Cloud Load Balancer. This includes an integrated Web Application Firewall (WAF). The purpose of the WAF is described later in this paper.

The Load Balancer directs connections to the Application Servers, distributing traffic across the span of available servers. The Load Balancer uses health probes to continuously check all Application Servers to ensure they are available. It will not direct connections to any Application Server it finds to be unresponsive.



MediaPulse Cloud Deployment

For Sky access, the Application Server then responds with a login page, requiring an authorized User Name and Password.

Client Side

There are three ways for a user to communicate with the MediaPulse Managed Cloud:

Method	***How***	***Why***
Sky	Connect to MediaPulse through a standard web browser. Xytech recommends using Chrome, Firefox or Safari for their superior performance.	No need to install client software on your device. Connect to MediaPulse using any device that supports a web browser.
SmartClient (SC)	Connect to MediaPulse through Xytech's proprietary client software	Use this access type to modify document layouts. Layout modification will be available in the Sky client in Version 9.
API	Connect to MediaPulse through Xytech's REST or SOAP API.	Utilize program-to-program communication for process automation.

All three methods provide access to the MediaPulse Managed Cloud and allow you to manage your personnel and inventory with speed and accuracy.

Authorization is conducted using OpenID Connect/OAuth Single Sign-On (SSO). Access to MediaPulse can be controlled through authentication provided by Azure OpenID Connect/OAuth. MediaPulse can also be integrated with other OpenID Connect/ OAuth providers.

- OpenID Connect/OAuth is only available through the Sky User Interface.
- OpenID Connect/OAuth provides a single location for password administration, control, and recovery.
- OpenID Connect/OAuth provides a layer of password security as passwords are not sent to MediaPulse over the public internet. Instead, the OpenID Connect/OAuth service validates a user's sign on and sends a token to MediaPulse that allows access to the user.

- For security purposes, each token has a specific lifetime and when the token expires, access to MediaPulse is revoked. This lifetime value is configurable within Azure's OpenID Connect/OAuth service.
- MediaPulse users created through the Microsoft Azure portal will be created automatically in MediaPulse along with their security roles, dashboards, and other user characteristics.
- MediaPulse users can still be created directly in the MediaPulse User Interface. They will also have to be created in the Azure OpenID Connect/OAuth service.

For API access, security credentials are carried in the connection request. These credentials are validated in the same manner as a User's Database or Windows login credentials. API calls with good credentials are allowed through, those with bad credentials are turned away. You control what actions may be accessed via the API through the API user role-based security within MediaPulse.

Using MediaPulse

User-to-Application:
Regardless of the access method used, once you have connected to the application you can now proceed to use MediaPulse. Whether by API or human activity, all actions are sent to the Application Server.

The Application Server holds onto the changes until it receives a command to save them. Once the Application Server receives the Save command, it passes those changes to the Database Server. Changes that are cancelled in the Application are not passed through.

Application-to-Database:
When MediaPulse is brought online, the Application Servers establish a secure session with the Primary Database Server. When using geo-replication, a Failover Database Server is added to the deployment and the Application Servers establish a secure session with them at the same time. The Primary and Failover Database Servers are each assigned a unique IP address and the IP Address is entered into an Authoritative DNS Server for resolution.

Changes entered into the Application Server are passed to the Primary Database Server and saved in the Database. Updates to the Primary Database are asynchronously replicated to the Failover Database automatically when geo-replication is used. Asynchronous replication means transactions are committed on the Primary Database before they are replicated to the Failover Database.

Part of the services provided by the DNS server is to check on the health of the Database Servers. When the DNS server discovers that the Primary Database Server is unavailable, it immediately routes all connections to the Failover Database. When the Primary Database Server has been brought back online, its database is synchronized with the Failover Database Server's database and DNS is manually shifted back to the Primary Database Server.

Storing Attachments in MediaPulse
MediaPulse offers the opportunity to add attachments to most anything, including Jobs, Work Orders, Assets, Titles, or Projects. These attachments are stored privately using Azure storage. One Hundred Gigabytes of storage is assigned to MediaPulse for this use, however this value can be increased. The use of non-Azure storage for attachments can be included in the design as an option. This option will require an Interface Adapter.

Staying Secure in the Cloud

Connecting to the MediaPulse Managed Cloud - whether using Sky or an API - may require your data to pass through the public internet. MediaPulse, as part of its deployment into the Azure Cloud, takes advantage of several security tools in order to keep your data secure while in flight and at rest.

CONNECTION SECURITY
Data security begins with the connection between the user's device and the Azure cloud.

- All connections to the MediaPulse Managed Cloud are established over a secure HTTP connection (HTTPS). This ensures all data in flight is securely encrypted and the application you are connected to is the application you requested. This prevents site spoofing and man-in-the-middle attacks.

- This same type of secure connection is used for all traffic between the MediaPulse application and database servers to encrypt that traffic, as well.

Azure VPN

A Virtual Private Network (VPN) is a connection method used to add security and privacy to private and public networks, letting you access the web safely and privately by routing your connection through a server and hiding your online actions. MediaPulse is deployed on the Azure Basic VPN, at our customer's request. A VPN may be needed for secure connections to outside systems such as on-premises storage for attachments or for connection to a third-party OpenID Connect/OAuth provider.

A useful analogy is that a VPN protects your data while on the web and a firewall protects your data while on the computer.

Firewalls

The term *firewall* is a metaphor that compares a type of physical barrier put in place to limit the damage a fire can cause with a virtual barrier put in place to limit damage from a cyberattack.

A firewall is software or firmware that enforces a set of rules about what data packets are allowed to enter or leave a network. Firewalls filter traffic and lower the risk of malicious packets traveling over the public internet impacting the security of a private network.

Two Types of Firewalls

A **Network Firewall** examines web traffic at OSI layers 3 and 4 and limits access to and from a device based on Source & Destination IP addresses, Port Numbers or packet types (TCP, Ping).

A **Web Application Firewall** (WAF) monitors, filters or blocks data packets as they travel to and from the application. It inspects each packet using a Rule Set, such as the ModSecurity core rule set covering the OWASP Top 10 vulnerabilities, to analyze OSI Layer 7 web application logic and block potentially harmful traffic such as Cross-Site Scripting (XSS) and SQL Injection attacks.

Xytech uses both of these firewall types to secure the MediaPulse Managed Cloud.

Azure Security

The Azure Cloud provides multiple security features[1] to mitigate threats against the MediaPulse application. These include:

1. Azure Networking: Azure requires virtual machines to be connected to an Azure Virtual Network. Each virtual network is isolated from all other virtual networks. This ensures network traffic in your deployment is not accessible to other Azure customers.

2. Network Access Control (NAC): Azure achieves this by limiting connectivity to and from specific devices or subnets within a virtual network. The goal of NAC is to limit access to your virtual machines and services to approved users and devices. Azure supports several types of NAC, including:
    a. Network Layer Control: Access controls are implemented in Azure through the use of Network Security Groups (NSGs) and are based on decisions to allow or deny connections to and from your virtual machine or service based on Source and Destination IP Address and Port along with the Protocol being used (TCP, UDP, etc.).
    b. Route Control: Azure networking supports the ability to customize the routing behavior for network traffic on your virtual networks. This enables you to alter the default routing table entries in your virtual network.
    c. Security Appliances: While NSGs and Route Control provide a level of security at the network and transport layers of the OSI model, you might also want to enable security at higher levels in the OSI stack. Such features as Intrusion Detection and Intrusion Response, URL Filtering, and Network Level AntiVirus/AntiMalware solutions are available.

3. Azure DDoS Protection[2]: Hackers and malicious groups are able to take temporary control of large numbers of Internet-based devices. They can then command these devices to start sending connection requests at a target, overwhelming both the network and the server causing severe service slowdowns and ultimately disabling the service. This type of attack is known as 'Distributed Denial of Service', or DDoS for short. Azure provides two levels of DDoS protection:

Basic: This level of Azure DDoS protection is used on the MediaPulse shared cloud and provides;

- Always-on traffic monitoring, which is automatically enabled at no additional charge and protects infrastructure and the Azure platform.
- Real-time mitigation of common network-level attacks, including automatic learning of per-customer traffic patterns at Layers 3 & 4
- Leveraging the scale of the Azure global network to distribute and mitigate DDoS attacks across regions, as the scale of Azure allows absorption of significant DDoS traffic, minimizing false positives.

Standard: This level of Azure DDoS protection is available to customers who opt for a private cloud solution. Standard DDoS protection:

- Includes all Basic features, including always-on monitoring, real-time attack mitigation, and attack distribution.
- Is designed to protect all resources and services deployed in a virtual network by applying three autotuned mitigation policies (TCP SYN, TCP, and UDP) for each public IP of the protected resource, in the virtual network with DDoS enabled.
- Understands customer environment resources and configuration, using protection policies tuned through dedicated traffic monitoring and machine learning.
- Mitigates over 60 different attack types, protecting against the largest known DDoS attacks - including Volumetric, Protocol and Application Layer attacks.
- Provides attack telemetry, alerting, and logging, allowing you to configure alerts for specific DDoS metrics to understand attack scale and other details.
- Includes attack simulation, which is available for validation of DDoS protections and incident response optimization.

4. Software Updates: As security issues are discovered and patched in system software, the updates have to be included in deployed systems. This requirement is addressed in the Managed Cloud.
    a) **Windows Updates:** Xytech monitors each server to ensure the latest patches are loaded monthly or earlier if recommended by Microsoft.
    b) **Database Updates:** Azure ensures each database has the latest version of patches.

Benefits of Deploying MediaPulse in the Azure Cloud

Microsoft rewrote SQL Server specifically for the cloud for great reasons. The database is implemented as 'Platform As A Service' (PAAS) and is only offered on Azure.

- **DESIGN:** Microsoft SQL database PAAS managed by Azure[3] is a complete development and deployment environment in the cloud. It includes infrastructure including servers and storage, networking, middleware, development tools, business intelligence services, and database management systems. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.
- **COST:** PaaS avoids the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware or the development tools and other resources. You manage the applications and services you develop, and the cloud service provider typically manages everything else.

  For example, operating in other Cloud services can require a purchase of MS SQL Server **PLUS** a fee to the Cloud operator to maintain the database. Paid updates or annual contracts are needed to maintain the current version. These fees do not apply when using the Xytech Azure solution.

- **BACKUPS:** Backups occur every 5 minutes[4]
  SQL Database automatically creates database backups.
  - Transaction log backups generally occur every 5 - 10 minutes.
  - Differential backups generally occur every 12 hours, with the frequency based on the performance level and amount of database activity.
  - Full database backups are created weekly.

  Transaction log backups, with full and differential backups, allow you to restore a database to a specific point-in-time to the same server that hosts the database. This is extraordinarily useful for restoring a corrupted database back to its last known-good point in time or for restoring a database that was accidentally deleted.

- **SUPPORT:** As Xytech is the MediaPulse expert we are able to offer much better support and quicker resolutions. If performance issues or problems occur, we have full access to witness and correct the issue quickly. Xytech has a debugger that can be connected to your instance. This allows our developers to easily track down issues not easily reproduced in our development environments.

- **SECURITY & PERFORMANCE:** Each customer has a separate secure private database instance that is not shared with other customers. This ensures other sites' traffic will not impact database performance. Xytech does not multi-tenant our customers' data.

- **XYTECH APP SERVER MONITORING:** Only Xytech can monitor the health of each app server. Every minute we check the health of each app server. Based on the severity email or phone calls are automatically sent to our Azure certified experts to remedy the issue 24 hours a day.

- **DATABASE MONITORING:** Proactive database analysis[5]
  Azure provides proactive database analysis through the Azure portal. SQL Database Intelligent Insights continuously monitors database usage through artificial intelligence and detects disruptive events causing poor performance. Once detected, a detailed analysis is performed and a diagnostic log is generated with an accurate assessment of the issue.

Identified SQL Database performance degradations are recorded in the diagnostics log with intelligent entries that consist of the following properties:

Property	***Details***
Database Information	Metadata about a database on which an insight was detected, such as a resource URI.
Observed Time Range	Start and end time for the period of the detected insight.
Impacted Metrics	Metrics that caused an insight to be generated: • Query duration increase [seconds]. • Excessive waiting [seconds]. • Timed-out requests [percentage]. • Errored-out requests [percentage].
Impact Value	Value of a metric measured.
Impacted Queries and Error Codes	Query hash or error code. These can be used to easily correlate to affected queries. Metrics that consist of either query duration increase, waiting time, timeout counts, or error codes are provided.
Detections	Detection identified at the database during the time of an event.
Root Cause Analysis	Root Cause Analysis of the issue identified in a human-readable format. Some insights might contain a performance improvement recommendation where possible.

Intelligent Insights analyzes SQL Database performance by comparing the database workload from the last hour with the past seven-day baseline workload. Database workload is composed of queries determined to be the most significant to the database performance, such as the most repeated and largest queries. Intelligent Insights also monitors absolute operational thresholds and detects issues with excessive wait times, critical exceptions, and issues with query parameterizations that might affect performance.

After a performance degradation issue is detected from multiple observed metrics by using artificial intelligence, analysis is performed. A diagnostics log is then generated with a specific description of what is happening with your database.

- **Advanced Azure security[6]:** Azure Security Center provides unified security management and advanced threat protection. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks.

  Azure Security Center provides the following Advanced Security features:

  - centralized policy management
  - actionable recommendations
  - advanced cloud defenses
  - continuous security assessment
  - prioritized alerts and incidents
  - integrated security solutions

- **Geo-Replication for High Availability[7]:** Geo-replication is available as an extra-cost option not included for all customers. It is an Azure SQL Database feature enabling database replication in the same or in a different data center (region) and is designed to allow the application to perform quick disaster recovery in case of a data center scale outage. If you are using active geo-replication and for any reason your primary database fails, or simply needs to be taken offline, you can initiate failover to your secondary database.

  Active geo-replication leverages the Always On technology of SQL Server to asynchronously replicate committed transactions on the primary database to a secondary database using snapshot isolation. While at any given point the secondary database might be slightly behind the primary database, the secondary data is guaranteed to never have partial transactions.

  Cross-region redundancy enables applications to quickly recover from a permanent loss of an entire datacenter or parts of a datacenter caused by natural disasters, catastrophic human errors, or malicious acts.

- **Redundant App & Web Servers with load balancing[8]:** Deploying MediaPulse in the Azure cloud leverages the ability to operate duplicate instances of Application and Web Servers. These are seen by users as a single resource. Duplicate server instances create redundancy in the deployment. The Load Balancer ensures that the load delivered to each Web/Application server pair is balanced. If one Web/Application server pair becomes non-responsive, it will be taken out of service in the Load Balancer until the issues can be identified and remediated. This ensures access to MediaPulse remains unaffected while issues affecting the individual server pair are addressed.

- **Encrypted data transfer[9]:** Azure offers many mechanisms for keeping data private as it moves from one location to another.

  Microsoft uses the Transport Layer Security (TLS) protocol, and SMB 3.0 in Virtual Machines (VMs) that are running Windows Server 2012 or later, to protect data when it's traveling between the cloud services and customers.

  You can use an Azure VPN gateway to send encrypted traffic between your virtual network and your on-premises location across a public connection, or to send traffic between virtual networks.

  - **Site-to-site VPNs** use IPsec for transport encryption.
  - **Point-to-site VPNs** utilize the Secure Socket Tunneling Protocol (SSTP) to create the VPN tunnel as it can traverse firewalls and appears as an HTTPS connection.

  Azure also provides encryption for 'data at rest' in its in-cloud storage. All data written to the Azure storage platform is encrypted through 256-bit AES encryption, one of the strongest block ciphers available. Handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to users.

- **API integration capabilities for any cloud or on-premises system:** MediaPulse supports XML-based SOAP APIs and, for release 8.3 and later, JSON-based REST APIs. These APIs are available for use on deployments in the Azure Cloud as well as in on-premises environments.

- **Three levels of managed services:** Xytech provides three levels of Managed Services to support MediaPulse deployed in Azure.

Level	*Services*
Base Services	Includes: • Management of the complete MediaPulse environment, • All Infrastructure Updates, • MediaPulse Updates, • Daily Database Backups, • Layout Maintenance, • A one-hour remote orientation for MediaPulse version updates.
Express Managed Services	Includes: • All Base Services, • User Management, • User Security Management, • Providing answers for non-support product questions, • Additional remote orientation for MediaPulse updates.
Full Managed Services	Includes: • All of the Base and Express services, • Performing MediaPulse Document Customizations and Layouts, • Extended orientation time for MediaPulse updates, • User and Security Role Management, • Management of all MediaPulse Setups and Preferences.

- **Complete product support for the MediaPulse software:** As the creator of MediaPulse Facility Management software, Xytech provides all support for it. This includes all enhancements, upgrades and problem resolutions.

- **Managed MediaPulse upgrades:** Xytech is constantly working to improve MediaPulse and introduction of these improvements are made on a controlled basis through Major and Service Pack releases.

  For Azure deployments, our team is responsible for installation of all MediaPulse upgrades. Whether you have purchased a license outright or are a subscriber to our service, your IT group is not responsible for ensuring a successful upgrade.

- **Worldwide private cloud available:** MediaPulse is deployed in Azure in several different regions, including:
  - Central United States
  - East Coast United States
  - Europe (France)

  Deploying in multiple regions ensures MediaPulse is protected against failures in a specific region due to an Azure facility event or a network connectivity problem in a specific site.

  Xytech uses shared VMs, where each customers' deployment of the MediaPulse application is created and maintained in a multi-client arrangement on a single instance of the MediaPulse application. In this case, through the use of login credentials, each customer's information is kept strictly separate from other tenants. Only the Application software is shared. Individual customer data is always kept private. This allows each customer to get the most value from MediaPulse while keeping costs down.

  For those customers with strict security requirements or other reasons why they cannot use the multi-client solution, a private cloud deployment can be set up with only their MediaPulse Application Server being deployed on the VM. There is a higher cost for this solution.

- **Vulnerability scans:** Xytech performs periodic vulnerability scans against the Azure network to ensure the security of MediaPulse on the platform. Using third-party scanning software, Xytech probes the Azure network for over 4500 known web vulnerabilities.

- **Web and mobile compatible:** As a cloud deployment, MediaPulse is accessible through Chrome, Firefox and Safari web browsers and can be reached through any device that supports these browsers, including PCs and Macs, Tablets, and Smartphones.

- **Single Sign-On (SSO) and OpenID Connect/OAuth authentication[10]:** MediaPulse supports the use of OpenID Connect/OAuth when using the Sky User Interface. OpenID Connect/OAuth allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.

  To support the use of Single Sign-On, additional configuration must be done for both the MediaPulse Application Server and the third-party OpenID/OAuth identity provider. Please note that a configuration fee will apply to integrate an OpenID/OAuth service other than Azure's OpenID Connect/OAuth.

  With OpenID/OAuth, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. This feature provides two key benefits:
  - Through the use of OpenID/OAuth, you only authenticate yourself once (Single Sign-On), to your OpenID/OAuth provider. This reduces the number of passwords you have to remember and the amount of time it takes to start using MediaPulse.
  - Other than your provider, no website ever sees your password, so you don't need to worry about the security of your password either at rest or in flight.

- **24x7 access and support:** Xytech recognizes that not having your facilities management software available to you can severely impact your ability to run your business. In the event of a Severity Level 1 or 2 problem, calling the Xytech Support number will put you in contact with Support personnel. During non-working hours your call will be routed to a Call Center that is available 24x7x365 and will be escalated to the appropriate support team member who will work with you to resolve your problem.

The Xytech Customer Portal provides a way to report problems of lesser severity on a 24x7x365 basis. Any issues you want to address can be entered into Xytech's trouble reporting system where they will be addressed.

- **Options:** Xytech has designed MediaPulse in the Azure cloud to accommodate the needs of a large segment of users through standard deployment offerings. Scattered through this paper are references to optional capabilities that can be included in the Azure deployment, at additional cost. In summary, these include:
    - Use of non-Azure OpenID/OAuth providers,
    - Attachment storage provided by Azure Storage services,
    - Attachment storage provided by your own, on-premises storage solution,
    - Azure Database GeoReplication,
    - Use of a Private Cloud solution on Azure.

Conclusion

Utilizing the Azure Cloud to run your MediaPulse application, rather than taking on the additional expenses related to hardware and software deployment coupled with internal ongoing maintenance and support, can lead to a more secure, flexible and reliable environment in which to operate. Taking advantage of this operating environment can increase uptime and secure sensitive data while keeping your business on track and moving forward. For more information, please contact Xytech at (818) 698-4900 or at www.xytechsystems.com.

Bibliography

[1]https://docs.microsoft.com/en-us/azure/security/security-network-overview

[2]https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

[3]https://azure.microsoft.com/en-us/overview/what-is-paas/

[4]https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automated-backups

[5]https://docs.microsoft.com/en-us/azure/sql-database/sql-database-intelligent-insights

[5]https://azure.microsoft.com/en-us/blog/automatic-intelligent-insights-to-optimize-performance-with-sql-data-warehouse/

[6]https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

[7]https://docs.microsoft.com/en-us/azure/sql-database/sql-database-geo-replication-overview

[8]https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

[9]https://docs.microsoft.com/en-us/azure/security/security-azure-encryption-overview

[10]https://OpenID Connect/OAuth.net/what-is-OpenID Connect/OAuth/