Innovation and Trends

Whitepaper: One-Time Passwords in Enterprise Cloud Environments

Fontys University
Javier Duran Caceres

Summary

This research will be investigating the use of one-time passwords in enterprise cloud architectures and compare the benefits to traditional use of password authentication. One-time passwords are temporary passwords created for a single usage and expire after a certain amount of time. They frequently serve as a type of two-factor authentication (2FA) on enterprise networks, especially in a cloud setting, to add an extra degree of security. The benefits of using OTPs in an enterprise network in a cloud environment include increased security and protection against cyber threats. Since OTPs are generated for a single use and expires in a short period of time, it makes it difficult for hackers to gain unauthorized access to the network, even if they have obtained the user's login credentials. Additionally, OTPs can be used as a second factor of authentication alongside a password, providing an additional layer of protection against password-based attacks. OTPs can also be used to authenticate users when accessing cloud resources from remote locations or on mobile devices, ensuring that the network is secure, regardless of the user's location.

Table of Contents

1. Introduction

As more organizations move their operations to the cloud, the security of enterprise networks has become a critical concern. Providing safe and convenient access to cloud resources for staff, partners, and clients is one of the largest difficulties facing businesses today. One of the most popular techniques for access control is still password-based authentication, although it is susceptible to several attacks, such as brute-force, phishing, and password guessing. One-time passwords (OTPs) are a potential solution to these challenges, providing an additional layer of security that can help protect against unauthorized access, data breaches, and cyber-attacks. This research paper will explore the use of OTPs in an enterprise cloud environment, examining the benefits, challenges, and best practices associated with implementing OTPs in a cloud-based network. The many OTP solutions that are available, their advantages and disadvantages, and the elements that companies should consider when choosing an OTP solution are also covered in the paper. This research paper seeks to assist enterprises in making knowledgeable decisions about their authentication procedures and strengthen the security of their cloud-based networks by offering a thorough overview of OTPs in an enterprise cloud context. During the investigation, Azure will be the main cloud provider to be researched.

2. Overview

2.1 Problem Definition

The problem to be solved is to find alternative solutions for traditional password uses such as OTPs as security threats increase. The issue with not utilizing OTPs in a corporate cloud network is that password-based authentication is no longer adequate to fend off the variety of current cyberthreats. Enterprise networks are susceptible to penetration by attackers who can access user credentials through a variety of methods, including phishing, social engineering, and brute-force attacks, if OTPs aren't used. Numerous detrimental effects, such as unlawful access to confidential information, monetary losses, and reputational harm to the company, may emerge from this. Additionally, several industries are required by compliance standards and laws to employ multi-factor authentication, so it is crucial that enterprises incorporate extra security measures like OTPs in their networks. In addition, it will enable employees from a company have a more secure access to remote services needed to perform their work, increasing availability and accessibility.

2.2 Project Goal

The goal of this research is to learn and understand One-Time Passwords as an alternative for traditional password authorization access. Using OTPs instead of traditional password authentication can achieve several goals, such as:

- Increased Security
- Compliance
- User Convenience
- Accessibility to remote services

Furthermore, the goal of this project is to learn the different tools and/or services offered by cloud providers, more specifically Azure in this case, to enable OTP solutions in cloud environments. In retrospect, using OTPs can help organizations achieve their security goals, comply with regulations, improve user convenience, and enhance their remote access capabilities.

2.3 Situation

During the project, the basic enterprise architecture recommended by Azure official documentation will be used as an example to implement an OTP solution. This reference architecture uses Azure Integration Services to orchestrate calls to enterprise backend systems. The backend systems can include software as a service (SaaS) system, Azure services, and existing web services in your enterprise. This architecture is sufficient for basic integration scenarios in which the workflow is triggered by synchronous calls to backend services. The intention is to research the implementation of OTPs in this network architecture as a proof of concept.

3. Research Questions

The research questions for this paper aim to explore the implementation of OTPs in an enterprise cloud environment and identify the challenges, benefits, and best practices associated with their use. By addressing these research questions, a comprehensive overview of the implementation of OTPs in an enterprise cloud environment will be done and intends to help organizations make informed decisions about their authentication strategies.

3.1 Main Question

- What is the effectiveness of implementing one-time passwords in enterprise networks within cloud environments for enhancing security and usability compared to traditional password-based authentication?

3.2 Sub Questions

1. What are the different one-time password authentication methods that can be implemented in an enterprise network within a cloud environment?
2. What are the benefits of using one-time passwords compared to traditional password based authentication in terms of security and usability?
3. How do one-time passwords affect the user experience and overall productivity of employees?
4. What are the potential risks and challenges associated with implementing one-time passwords in enterprise networks within cloud environments?

4. Research Methodology

The research methodology section of this paper describes the approach used to answer the research questions and achieve the objectives of the study. In this section, the DOT framework will be taken into consideration to perform the investigation. The strategies or methods that will be used during this research are mostly library and lab strategies.

4.1 One-Time Passwords

In this subchapter, the sub question "What are the benefits of using one-time passwords compared to traditional password-based authentication in terms of security and usability? " will be answered.

One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once (THALES, 2023). Usually, OTPs expire after a period of time to avoid password leaks and increase security. They are often used as a form of two-factor authentication (2FA) to provide an additional layer of security in enterprise networks, particularly in a cloud environment. The benefits of OTPs are mostly security related, but it also increases the availability of remote services. Using OTPs in an enterprise cloud network can provide multiple benefits such as:

- Security: OTPs add an additional layer of security to the authentication process by requiring a unique one-time code in addition to a traditional password. Making it more difficult for attackers to gain access through password attacks such as password cracking, brute force attacks or even password guessing.
- Compliance: Many regulations and compliance requirements mandate the use of multi-factor authentication. OTPs can be used as a method of 2FA, making sure these regulations are met.
- Improved Employee Experience: OTPs are easy to use and do not require users to remember complex passwords or use password managers. In addition, employees will have a secure way to access remote services.
- Remote Access: OTPs can be used as a second factor of authentication for remote access to cloud resources, this will decrease the possibility of unauthorized users in the network.
- Reduce Risks: Using OTPs reduce the risk of some attack vectors, such as data leaks and data breaches, password attacks, between others. In other words, reduces the risk of data breaches and protects sensitive information.
- Password Management and Issues: Implementing OTPs can reduce IT costs associated with managing password resets and other password-related issues.
- Easy Integration and Scalability: OTPs are a great option for Enterprise Cloud networks that need to handle a large number of users since they can be readily scaled to suit the needs of growing enterprises. (SINCH, 2022)

4.2 Azure

Azure is a leading cloud provider that offers a wide range of cloud-based services to businesses of all sizes. According to Microsoft, over 95% of Fortune 500 companies use Azure to power their operations, including enterprise applications, data analytics, and artificial intelligence (AI). Azure has a global presence, with data centers located in over 60 regions across the world, providing high availability and low-latency services to customers. Azure offers a wide range of cloud-based services, including, among others, virtual machines, storage, databases, analytics, artificial intelligence, and the Internet of Things. Additionally, it offers sophisticated security and compliance capabilities, like as multi-factor authentication, network security groups, and data encryption, to assist businesses in safeguarding their data and cloud-based applications. Azure is also a popular choice for enterprises to operate in the cloud due to the easy implementation of hybrid environments for enterprises (Microsoft, 2022). Azure will be the focus of this research because it is a highly used cloud provider across different companies, and I would like to increase my knowledge on this cloud provider and the possibilities it has when it comes to alternatives for traditional password authentications.

4.3 Azure OTP Methods and Services

In this subchapter, the sub question “What are the different one-time password authentication methods that can be implemented in an enterprise network within a cloud environment?” will be answered.

As a growing cloud provider for enterprise uses, Azure has developed several tools and methods to implement 2FA and/or OTPs in a network architecture. Azure provides several methods to implement OTPs in an enterprise cloud environment, such as:

- Azure Active Directory: Azure Active Directory (Azure AD) supports the implementation of One-Time Passwords (OTP) as an additional layer of security for user authentication. Azure AD can use Conditional Access is a policy-based access control feature that allows administrators to define access policies based on various criteria, such as user location, device type, or application. Administrators can use Conditional Access to require users to authenticate with an OTP before accessing specific resources or applications.
- Azure MFA: Azure MFA is a cloud-based multi-factor authentication service that supports the use of OTPs. With Azure MFA, users can authenticate using OTPs delivered through a mobile app, text message, or phone call. Azure MFA also supports other authentication methods, such as smart cards, biometrics, and one-way SMS (Microsoft, 2022).
- Azure AD B2C: Azure AD B2C is a cloud-based identity management service that supports OTP authentication for customer-facing applications. Azure AD B2C provides several options for implementing OTPs, including using the Microsoft Authenticator app or text messaging.
- Azure Key Vault: Azure Key Vault is a cloud-based service that allows organizations to securely store and manage cryptographic keys and secrets, including OTP secrets. Azure Key Vault provides a secure way to generate and manage OTP secrets and integrate them into authentication workflows.

4.4 Azure Enterprise Network

In Figure 4.4.1, the diagram shows the network architecture that is being researched in this case. The architecture is the basic enterprise integration on Azure as mentioned in the official Azure documentation (https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/enterprise-integration/basic-enterprise-integration).

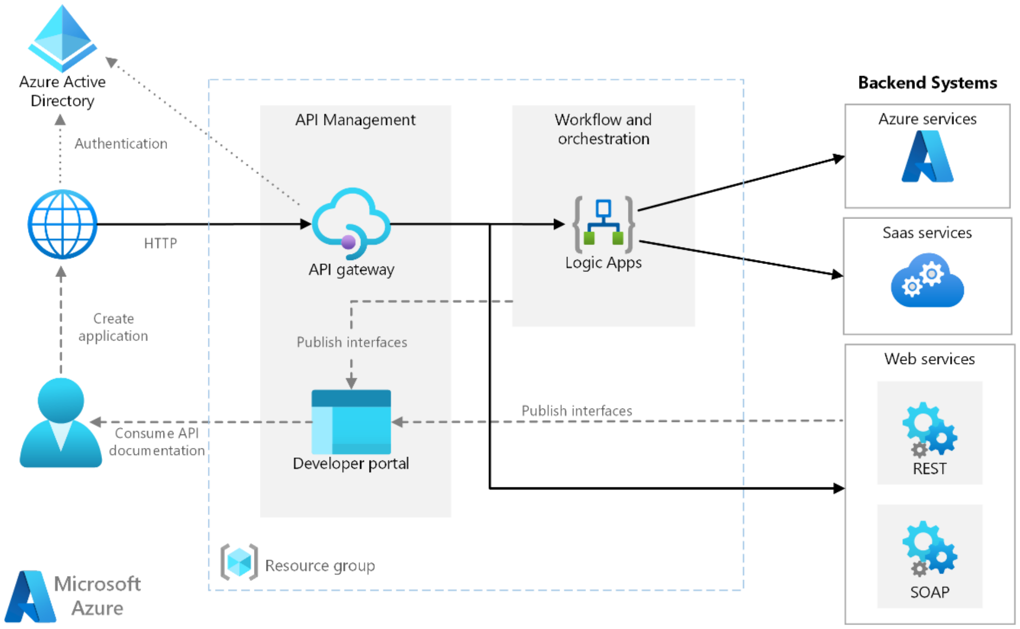

Figure 4.4.1

Workflow

- Backend Systems: The diagram's right side lists the many backend systems that the company has implemented or depends on. SaaS systems, additional Azure services, or web services that expose REST or SOAP endpoints may be among these systems.
- Azure Logic Apps: In this architecture, logic apps are triggered by HTTP requests.
- Azure API Management: fully managed service offered by Microsoft Azure that provides a way to publish, secure, manage, and analyze APIs (Application Programming Interfaces). With Azure API Management, developers can easily create and expose APIs to internal or external developers, partners, or customers.
- Azure DNS: Azure DNS provides name resolution by using the Azure infrastructure.
- Azure Active Directory: is a cloud-based identity and access management service offered by Microsoft Azure. It provides a way to manage and control access to cloud-based and on-premises applications, resources, and services (Microsoft, 2023).

4.5 Solution

The architecture shown in the previous chapter (Figure 4.4.1) contains an Active Directory and is considered the basic enterprise integration by Azure. To allow employees and/or clients to access all the necessary services to perform their job or access crucial data securely there are a few ways to implement OTPs in this Azure architecture. The possible solutions are:

- **Azure Multi-Factor Authentication (MFA)**

Azure MFA is a cloud-based multi-factor authentication service that supports the use of OTPs as an additional layer of security for user authentication. With Azure MFA, users can authenticate using OTPs delivered through a mobile app, text message, or phone call. Azure MFA also supports other authentication methods, such as smart cards, biometrics, and one-way SMS.

- **Azure AD Conditional Access**

A policy-based access control tool called Azure AD Conditional Access enables administrators to specify access controls based on several factors like user location, device type, or application. Administrators can use Conditional Access to make it necessary for users to authenticate with an OTP before using a certain application or resource. Only authorized users will have access to sensitive data and apps thanks to conditional access restrictions, which may be tailored to the unique needs of the organization.

- **Microsoft Authenticator App**

An OATH verification code can be generated using the Authenticator app as a software token. You enter the code generated by the Authenticator app into the sign-in interface after providing your username and password. A second method of authentication is offered via the verification code.

Furthermore, each implementation method uses different authentication methods to ensure security when using MFA or OTPs. The following table outlines the security considerations for the available authentication methods (Microsoft, 2023). Availability is an indication of the user being able to use the authentication method, not of the service availability in Azure AD:

Authentication Method	**Security**	**Usability**	**Availability**
Windows Hello for Business	High	High	High
Microsoft Authenticator	High	High	High
Authenticator Lite	High	High	High
FIDO2 Security Key	High	High	High
Certificate-based Auth	High	High	High
OATH Hardware Tokens	Medium	Medium	High
SMS	Medium	High	Medium
Voice	Medium	Medium	Medium
Password	Low	High	High

In retrospect, these 3 methods mentioned before are the best options to implement OTPs or OTPs as a 2FA or MFA authentication for an Azure architecture containing an Active Directory.

4.6 Potential Risks

In this subchapter the sub question "What are the potential risks and challenges associated with implementing one-time passwords in enterprise networks within cloud environments?" will be answered.

While implementing OTPs in enterprise networks within cloud environments can enhance security and usability, there are also potential risks and challenges to consider. First of all, OTPs may not be compatible with all devices or applications, which could limit their usefulness in some situations. There are also potential security risks associated with implementing OTPs. Furthermore, OTPs provided by SMS, for instance, may be intercepted and compromised, potentially allowing unwanted access to critical information. OTPs produced by mobile apps may also be susceptible to malware or other sorts of attacks. Finally, the requirement for efficient management and monitoring of OTPs presents another difficulty. Organizations may occasionally need to make additional infrastructure investments to enable OTPs and make sure they are appropriately managed and monitored.

5. Conclusion

In conclusion, the use of OTPs in enterprise networks within cloud settings can, in comparison to conventional password-based authentication, dramatically improve security and usability. Because OTPs are created for each authentication attempt and are difficult to guess or reuse, they are more secure. This makes it far more difficult for hackers to access critical data and company networks without authorization. Additionally, OTPs are more user-friendly because they do not require users to remember and manage multiple complex passwords. Instead, users can authenticate quickly and easily using a mobile app, text message, or phone call. Implementing OTPs in an Azure enterprise cloud environment with an Active Directory can be done through Azure MFA, Microsoft Authenticator App and Azure AD Conditional Access, both of which provide a high level of security and flexibility for authentication. In addition, OTP implementation in enterprise networks within cloud settings is often beneficial, and businesses should think about using this strategy to improve security and usability and service availability to be able to perform the work.

References

Microsoft. (2022). *How to MFA Settings?* Retrieved from Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Microsoft. (2022). *What is Azure?* Retrieved from Microsoft: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

Microsoft. (2023). *Basic Enterprise Integration on Azure.* Retrieved from Microsoft: https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/enterprise-integration/basic-enterprise-integration

Microsoft. (2023, March 15). *What authentication and verification methods are available in Azure Active Directory?* Retrieved from Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

SINCH. (2022, July 18). *What is a one time password (OTP)? Features and benefits explained.* Retrieved from SINCH: https://www.sinch.com/blog/one-time-password/

THALES. (2023). *One Time Password.* Retrieved from THALES Group: https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp#:~:text=What%20does%20OTP%20mean%3F,method%20and%20the%20least%20secure.