THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE12

PUBLISHED DATE: - 11-12-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue12-07 **PAGE NO.: - 59-67**

RESEARCH ARTICLE **Open Access**

IMPLEMENTING COMPREHENSIVE IDENTITY CONTINUITY PLANS TO COUNTERACT CYBER THREATS

Raoul Hira
Principal Security Consultant, Vistra USA

Abstract
The article examines the study of methods for implementing integrated identification continuity plans to counter cyber threats and outages with third parties. The study focuses on the analysis of various types of authentication failures, their implications for data security and business processes, as well as their impact on user experience. Approaches to the use of backup authentication and multi-factor authentication (MFA) providers, and continuous monitoring to increase the level of security are considered. The analysis demonstrates the need for regular testing of systems, the introduction of backup mechanisms to prevent failures, and risk assessment. The article also describes the importance of integrating modern solutions into an authentication system to minimize threats and maintain the continuous operation of key processes. The study highlights the importance of an integrated approach to ensuring data identification and protection in the context of modern cyber threats.

Keywords cyber threats, authentication, backup providers, multi-factor authentication, continuity of identification, business continuity, information security.

INTRODUCTION

In the context of the rapid growth of digitalization and the increasing number of cyber threats, ensuring data security becomes a key factor in the successful operation of companies. One of the most vulnerable areas in information security is the process of user authentication and identification. Modern cyberattacks are often aimed at compromising credentials, which can lead to the leakage of confidential information and disruption of normal system operations. To improve authentication security and reduce friction with applications many organizations have chosen to leverage cloud based authentication providers. This has now become a single point of failure. In this regard, the development and implementation of comprehensive plans for ensuring continuous identification become critically important for protecting business processes and maintaining customer trust.

The relevance of this topic is driven by the need to improve the reliability of identification systems, which directly affects companies' resilience to cyberattacks or a misconfiguration leading to failure of the authentication provider. Authentication errors, whether caused by technical failures or malicious actions, can significantly reduce the efficiency of business processes, ultimately leading to financial losses and a decline in the company's reputation. As a result, many organizations are seeking to architect their most critical systems to minimize the risks associated with authentication failure through the

implementation of backup authentication and multi-factor authentication (MFA) providers, and continuous security system monitoring.

The objective of this study is to analyze and evaluate methods for implementing comprehensive identification continuity plans to counter cyber threats, failure of primary identity providers, as well as to identify key factors influencing the effectiveness of these plans.

1. Consequences of Authentication Service Downtime

Authentication process failures can be characterized as malfunctions that occur during the verification of user data required to grant access to the system. Downtime in the authentication service can lead to serious consequences for the system, disrupting user access to key applications or platform functions. Primarily, this can result in access being blocked for both internal and external users, negatively affecting employee productivity and customer satisfaction. In the case of commercial platforms, downtime can result in revenue loss, especially if users are unable to complete transactions or access important services. Additionally, it creates security vulnerabilities, as users may resort to unsafe methods to bypass authentication. Authentication service downtime can also impact a company's reputation, undermining trust in the system's reliability [1].

However, even the most advanced infrastructures are susceptible to failures, which can have significant consequences for both users and businesses as a whole. Analyzing real cases of authentication service downtime allows for a deeper understanding of the nature of such incidents, their impact on system operations and users, and the identification of potential preventive measures to avoid similar situations in the future. Reviewing these cases can serve as a foundation for developing more resilient solutions in the field of authentication and data security.

For example, on November 15, 2022, at 10:37 AM Pacific Time, Okta released an integration update with Microsoft Office 365 to remove outdated links to Microsoft Dynamics. At 11:09 AM the same day, reports of authentication failures via SSO in Microsoft Office 365 began to surface. Upon analyzing the situation, it was determined that the issue affected all clients using Office 365, and users were presented with a message stating that the "federated realm object does not exist."

It was established that the issue arose from a change in Okta's code, which was implemented as part of a standard update process. Moreover, Okta used its internal service to update the metadata of third-party integrations. At 10:37 AM, using this service, obsolete links to Dynamics 365 applications were removed, leading to authentication failures for clients using domain federation without initialization.

In an attempt to fix the issue, several attempts were made to clear the application-level cache, but these efforts were unsuccessful. At 4:25 PM, Okta rolled back the configuration, but this did not restore the system since the earlier changes had deleted important objects. After further analysis of the problem, clients were advised to reconfigure their federated domains to resolve the issue.

On November 16, Okta released guidance for clients to resolve the authentication issue in Microsoft Office 365. Despite efforts to find a solution that did not require client action, the optimal option turned out to be a manual reconfiguration of the domains.

To prevent similar incidents in the future, the following steps were outlined: temporary suspension of configuration deployment to conduct internal audits, phased implementation of changes to application metadata, enhanced testing of the configuration deployment system,

improvement of the change validation process, and the development of an error alert system at the testing stage [3].

Between 05:17 and 05:42 Pacific Time on October 12, 2023, Okta engineers identified internet connectivity failures that affected a specific group of customers in the United States using commercial cells. According to monitoring data, connectivity errors to commercial cells in the United States were recorded on October 7 at 12:36 and on October 12 at 05:17 Pacific Time. These failures resulted in the inability of some users to connect to the Okta service depending on their location.

The analysis of the situation showed that the failure was caused by issues in the service provider's network infrastructure, leading to Okta being inaccessible through several points of presence (PoP). This incident caused connection errors to the service, although outgoing requests to Okta remained unaffected.

To prevent similar situations in the future, Okta has strengthened its collaboration with the service provider to ensure timely communication with customers and prompt resolution of potential issues. Additionally, the company is revising its procedures for monitoring and detecting network errors to improve reliability and response speed to such incidents. The total duration of the incident was 25 minutes [3].

On August 15, 2022, Duo experienced a significant outage affecting its Single Sign-On (SSO) product across multiple deployments. The incident began around 8:00 EDT when Duo's Engineering Team was alerted to degraded performance in the SSO service. The root cause was identified as a recent configuration change to increase observability capabilities, which unexpectedly caused the software to consume excessive resources, leading to cascading failures. The issue impacted numerous deployments, causing authentication failures and 504 Bad Gateway errors for SSO-protected applications and the Duo Admin Panel. Duo's Site Reliability Engineering (SRE) team worked diligently to resolve the problem, attempting various solutions including restarting instances, clearing database call backlogs, rolling back software versions, and scaling up infrastructure. The root cause was ultimately identified and fixed by 11:21 EDT, with the issue fully resolved by 14:46 EDT. Duo implemented several measures to prevent future occurrences and improve response times, including enhancing monitoring capabilities, refining change management processes, and updating status page procedures [4].

On August 13, 2023, Ping Identity experienced a global outage affecting its PingID Service. The incident, detected by monitoring systems, caused the service to be unavailable for approximately 12 minutes, from 10:13 to 10:25 UTC. The outage impacted PingID services across multiple regions, including Europe (.eu services), Australia (.com.au services), and the United States (.com services), affecting both PingID Authenticator and PingID Server components. Ping Identity promptly identified and resolved the issue, restoring normal service operations [5].

To prevent similar failures, Okta continues to work closely with external service providers to ensure timely client notifications and prompt resolution of potential issues [6].

It can be stated that authentication errors can negatively affect both users and the company. Failed access attempts can cause frustration among users, especially when they are in a hurry or rely on the quick completion of tasks through the application. This is particularly evident in financial systems, where speed is critical.

In more severe cases, where a malicious actor gains access to restricted data, the consequences can be even more destructive. This leads to the leakage of confidential information and

undermines client trust in the company, ultimately reflecting poorly on its reputation. In the long term, this erodes trust in the company and damages its reputation.

2. The Need for Secondary Authentication Providers

In the context of digitalization and increasing data security demands, authentication becomes a key element in ensuring business continuity. The implementation of authentication systems, especially with the involvement of secondary providers, allows companies to minimize risks associated with potential failures or threats in the primary authentication system. Secondary authentication providers can serve as backup solutions, ensuring access to corporate resources in the event of a failure in the primary system or when critical vulnerabilities are identified.

Corporate access control, in turn, is based on an identity provider (IdP) that connects to applications using federation technologies such as SAML and OpenID Connect. At the same time, protocols like SCIM allow for provisioning and de-provisioning access to applications, while users and devices are managed through a central control panel. Meanwhile, HR systems store employee lifecycle management information and exchange it to ensure a consistent representation of access.

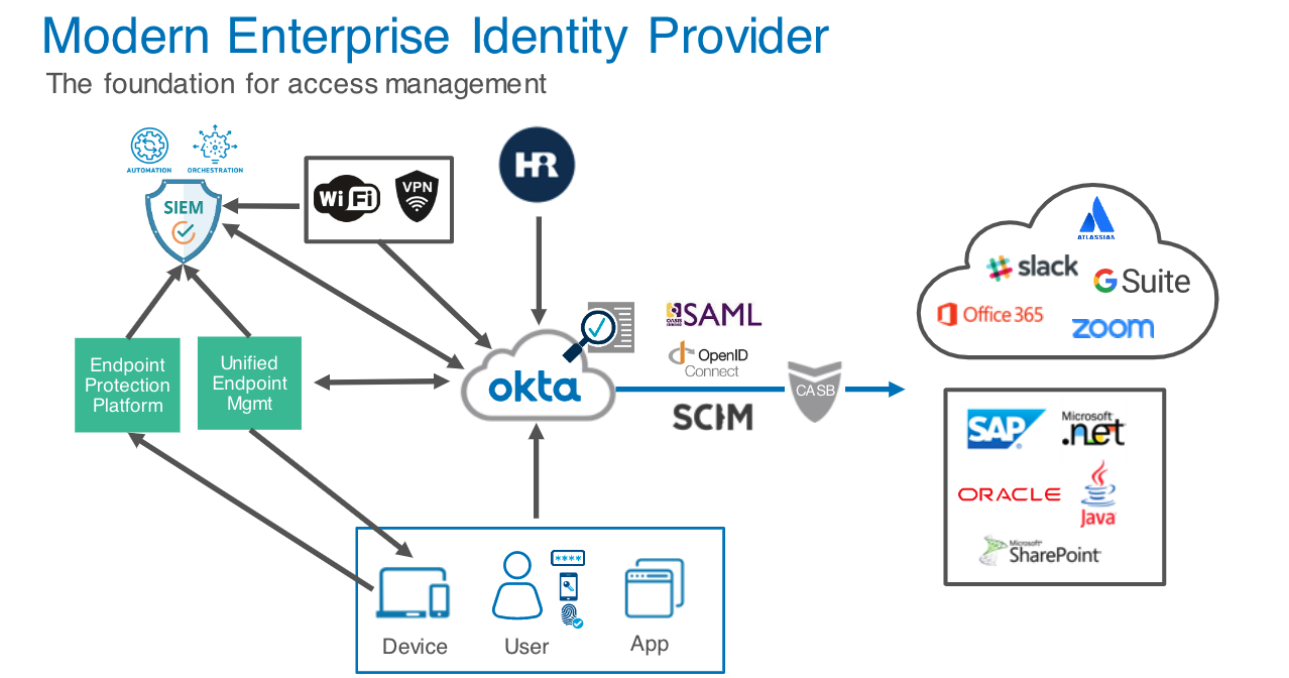

Fig.1. Modern Enterprise Identity Provider [7]

The integration of corporate identity management systems (IdP) is becoming increasingly essential for securing access to networks via Wi-Fi and VPN. It also interacts with endpoint management solutions to ensure that only trusted devices are granted access. This approach to identity management can be further supported by security information and event management (SIEM) systems and session control technologies, such as single sign-on (SSO).

In this system, there is a shift in the authentication model from the traditional "connect then authorize" approach to a "first authorize, then connect" model. Authentication decisions are

made based on device analysis, user identity verification, and the results of federated authentication mechanisms. Most modern identity providers are not fully capable of accounting for all contextual aspects and are forced to request re-authentication if background verification fails.

Companies seeking to enhance security require solutions that allow for continuous user access evaluation without degrading the user experience. In this regard, the concept of continuous authentication comes to the forefront.

The approach to continuous authentication relies on the use of various data, such as geolocation information, Bluetooth signals, or biometric parameters, including Face ID, to passively verify access to resources. The use of long-term security identifiers helps maintain constant access without the need for user interaction. The development of this method has been made possible by the introduction of standards like FIDO Alliance and WebAuthn, which have created an ecosystem of modern authenticators using advanced technologies. The standardization of device security assessment processes also plays a significant role in this.

Since continuous authentication relies on extended identification sessions, an effective approach to managing changes in these sessions is necessary. Although the issue of long sessions has existed for some time, it has become more complicated with the advent of new use cases and the diversity of clients, including mobile applications, cloud solutions, Internet of Things (IoT) devices, APIs and Zero Trust.

Modern applications are often developed with the platform's native capabilities in mind. An example is the Slack application, which requires authentication only at the first launch, after which it operates in the background, providing access to corporate resources like Google Drive or Dropbox.

These applications often use the OAuth 2.0 protocol, allowing access tokens to be automatically refreshed and enabling interaction with APIs without requiring the user to re-enter their credentials. However, this architecture creates certain challenges for continuous authentication, as IdP systems do not always control verification processes within OAuth, limiting the ability to establish a reliable context for applications and devices.

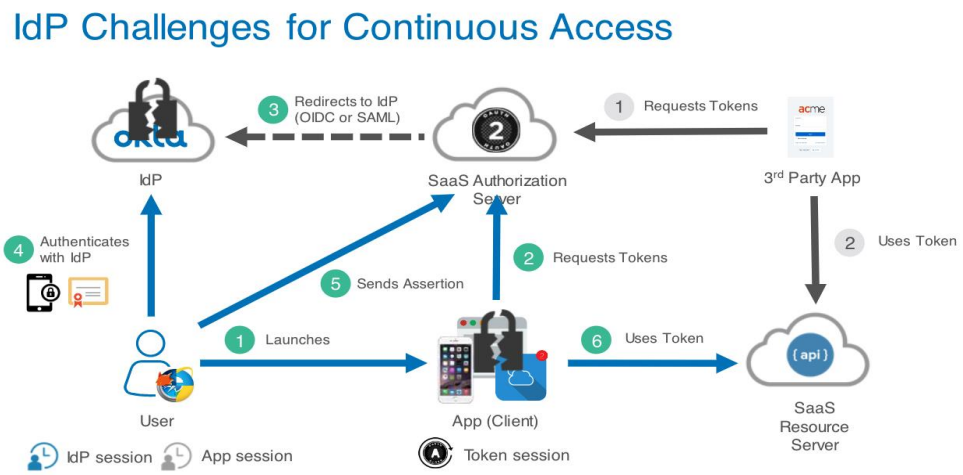

Fig. 2. IdP challenges for continuous access [7].

Additional challenges faced by temporarily displaced persons (IdP) include the following aspects:

• Policies governing user identification and authentication (IdP) are applied exclusively within the single sign-on (SSO) system, with no standard interface for revoking or reassessing access.

• In the case of extended sessions, the risk level may change after the authentication procedure has been completed.

• As SaaS solutions increasingly transform into integrated platforms, IdP cannot often interact with connected applications and services [7].

The use of third-party authentication providers also helps manage peak system loads. During periods of increased user activity, such as sales or the launch of a new product, backup systems ensure stable business operations, avoiding downtime and maintaining a high level of customer service. This is especially crucial for companies operating under high demands for data availability and security [8].

Moreover, secondary authentication providers contribute to the overall security of the system. If the primary system is compromised or becomes unavailable, backup providers can temporarily take over data protection and access control functions, thereby preventing data breaches and disruptions to business processes

Next, Table 1 will describe the advantages and disadvantages of implementing additional authentication providers.

Table 1. Advantages and disadvantages of implementing additional authentication providers [9].

Advantages	Disadvantages
Increased security: Using multiple authentication providers can enhance system protection by adding extra layers of security.	Complexity in management: Managing multiple authentication providers can lead to increased system administration complexity.
Flexibility for users: Users can choose their preferred authentication provider, which may improve their experience with the system.	Increased costs: Implementing and maintaining additional providers may require significant financial and resource expenditures.
Improved availability: Supporting multiple providers allows for broader access to the system across different platforms.	Compatibility issues: Not all providers may integrate seamlessly with each other or with existing systems.
Reduced dependency on a single provider: The organization is not reliant on a single solution, reducing risks associated with service outages or policy changes.	Increased authentication complexity: Users may become confused when selecting an authentication provider, which could degrade their experience.
Regulatory compliance: Using multiple providers can help meet data security regulatory requirements in different regions.	Need for additional training: Administrators and users may need time to adapt to new authentication mechanisms.

Thus, the necessity of using secondary authentication providers is driven by the fact that

they provide an additional level of protection and stability for business processes. These providers help minimize risks related to data breaches, hacks, and security system failures, which is particularly important given the growing threats in the digital economy. Through authentication system redundancy, in the event of a failure or compromise of the primary system, secondary providers can immediately assume access control functions, ensuring continuity of operations and data protection..

3. Recommendations for Ensuring Identification Continuity to Counter Cyber Threats

To effectively manage risks, continuity plans must be regularly updated. These plans should clearly define target recovery point objectives (RPO) to determine an acceptable level of data recovery, as well as recovery time objectives (RTO) for key authentication services. Applications should be prioritized based on their criticality, including the possibility of utilizing backup providers. For high-risk scenarios, it is recommended to develop detailed authentication strategies.

When analyzing backup authentication services, it is essential to consider their compatibility with the existing infrastructure and current providers. Additionally, the reliability, security, and compliance of the selected providers should be assessed. The geographical location of providers plays a key role in minimizing data transmission delays.

Cost assessment for the implementation and operation of additional providers is a crucial part of the planning process. Resources, including personnel, technology, and training, must be allocated. A cost-benefit analysis will help justify investments in ensuring authentication continuity.

To comply with legal regulations and standards in the field of authentication and data protection, it is important to carefully examine applicable laws. The selection of providers should take into account their compliance with data storage and processing requirements.

A phased implementation approach minimizes risks. It is recommended to test changes on less critical systems during the initial stages, and then gradually roll them out to key applications. This process requires careful planning and adjustments based on interim results.

To ensure secure operations, it is necessary to configure data synchronization between the primary and backup providers, as well as automatic failover in case of disruptions. Establishing a reliable connection between the primary and backup infrastructure is critical.

To ensure system reliability, monitoring tools covering both primary and backup components must be implemented. These systems should check the status, and performance, and maintain centralized logs, providing automatic notifications for prompt incident response.

Regular testing of failover and recovery scenarios is essential for verifying the readiness of backup services. Tests should include procedures for switching and recovering critical applications.

All processes related to ensuring authentication continuity must be documented. Developing detailed recovery, failover, and maintenance procedures, as well as incident response plans, is a mandatory step.

For effective management of authentication systems, regular employee training is required, along with providing users with up-to-date instructions on evolving processes.

Setting up failover processes between the primary and backup providers to minimize risks and optimizing data synchronization improves the overall efficiency of the system.

Continuous risk analysis, testing of procedures, and improving authentication processes enhance system stability and security. Feedback from users helps identify and eliminate weak points.

Continuous monitoring of authentication systems and backup services, with the use of analytical dashboards for visualizing system status, enables rapid incident response. Regular testing of failover scenarios increases preparedness for unexpected situations.

The implementation of change management systems and regular internal audits ensures compliance with security requirements and helps demonstrate this during external inspections.

Regularly train users about authentication processes and supporting them increases satisfaction including setting up alternative MFA provider for the secondary provider. Collecting feedback from users contributes to the improvement of the authentication systems and processes.

Regular recovery tests simulating various failure scenarios help identify potential system vulnerabilities and address them promptly.

Thus, constant attention to performance, security, and the quality of the user experience reduces risks and contributes to the sustainable operation of authentication systems.

CONCLUSION

The implementation of comprehensive identification continuity plans plays a crucial role in countering cyber threats. An authentication system supported by backup providers and multi-factor authentication helps minimize risks related to data breaches and system failures. Regular audits, monitoring, and testing of failure scenarios enhance the reliability and security of systems, which in turn strengthens user trust and reduces the likelihood of successful cyberattacks. A strategic approach to the adoption of such solutions requires not only technological modernization but also organizational efforts focused on compliance with regulatory standards and employee training.

REFERENCES

1. Wang D. et al. Understanding security failures of multi-factor authentication schemes for multi-server environments //Computers & Security. – 2020. – Vol. 88. – p. 101619.
2. Microsoft O365 Federation SSO issue. [Electronic resource] Access mode: https://status.okta.com/#incident/a9C4z000000Yzi5EAC (accessed 08/31/2024).
3. Okta Connectivity Disruption for Some US Customers. [Electronic resource] Access mode: https://status.okta.com/#incident/a9C4z000009wkeEAA (accessed 08/31/2024).
4. Multiple Deployments: Single Sign-On Connectivity Errors. [Electronic resource] Access mode: https://status.duo.com/incidents/p1xdjgy4sj07(accessed 08/31/2024).
5. PingOne Service Interruption. [Electronic resource] Access mode: https://status.pingidentity.com/incidents/vsrhzjxhvn8s(accessed 08/31/2024).
6. Single Sign-On Issues for Microsoft O365 OneDrive. [Electronic resource] Access mode: https://status.okta.com/#incident/a9C4z000000TXIOEA4 (accessed 08/31/2024).
7. Strelets A. I. et al. Multi-user System For Remote Work with Programmable Devices //2024 Conference of Young Researchers in Electrical and Electronic Engineering (ElCon). – IEEE, 2024. – pp. 83-85.

8. Shirvanian M., Agrawal S. 2D-2FA: A new dimension in two-factor authentication //Proceedings of the 37th Annual Computer Security Applications Conference. – 2021. – pp. 482-496.

9. Okta Authentication: Streaming Access with Secure Identity Management. [Electronic resource] Access mode: https://www.cloudally.com/glossary/okta-authentication / (accessed 08/31/2024).