Gemalto’s SafeNet Authentication Service support in IBM Multi-Factor Authentication for z/OS Helps Maintain a Secure Infrastructure

An explosion of malicious attacks of increasing sophistication on computer systems has occurred recently. According to the 2017 Verizon Data Breach Investigations Report, there were 1,935 of these last year alone and growing. Sixty three percent were due to weak, default or stolen passwords and a whopping 60% were from the inside. It seems like you hear about another attack every week. The increased use of low-cost and powerful password cracking systems has made attacks much easier, placing the burden on organizations to increase their levels of defense.

Mobile and cloud architectures make it imperative to reduce the risk of external threats, raising questions about the adequacy of password protection. Criminals are targeting employees at organizations and exploiting them with savvy phishing attacks, malware, key logging, or password cracking to steal their logon credentials. If this user has access to private customer information as part of their job, the criminal has access to the corporate jewels (e.g., social security numbers, health records, etc.). Many users use passwords with common defaults that are easily guessed, reuse them, or write them down. Cyber criminals know that.

Password vulnerabilities were named in several high-profile hacks in recent years, and the 2017 Verizon Data Breach Investigation Report (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/) states that use of stolen credentials or weak passwords has become a top threat.

Gemalto's SafeNet Authentication Service support in IBM Multi-Factor Authentication for z/OS® raises the assurance level of user authentication to z/OS applications and hosting environments by allowing the use of multiple authentication factors.

Gemalto's SafeNet Identity and Access Management Solutions

Gemalto's SafeNet Identity and Access Management solutions enable enterprises across many verticals, including major financial institutions and governments, to utilize access management, PKI credential management, and strong authentication and identity management solutions to secure access to sensitive resources and protect digital interactions. Supported authentication methods include context-based authentication combined with step-up capabilities, Out-of-band (OOB), one-time password (OTP) and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.

Gemalto's SafeNet Authentication Service offers fully automated authentication delivered from the cloud to raise the assurance level that a user is who they claim to be, ensuring secure access to critical applications and data, with OTP-based strong authentication, whether using a hardware keyfob, mobile device, or grid-based authenticator. Since SafeNet Authentication Service is managed by Gemalto in the cloud, it offers numerous cloud efficiencies, including significantly lower implementation and ongoing administration and maintenance costs. Included in the SafeNet Authentication Service subscription price is one hardware token, the SafeNet OTP 110, or one software token, the SafeNet MobilePASS+ next-generation OTP app. The SafeNet OTP 110 is a compact and portable strong authentication device that allows organizations to conveniently and effectively establish OTP-based access control (see figure 1), to any enterprise resource.

Figure 1: SafeNet OTP 110 token

SafeNet MobilePASS+ (figure 2) is a next generation software token that offers secure one-time passcode (OTP) generation on mobile devices, as well as single-tap push authentication for enhanced user convenience. Featuring QR code enrollment and biometric fingerprint PIN on mobile devices, the MobilePASS+ app offers frictionless authentication for users, as well as simple management and out-of-the-box integration with a broad range of enterprise resources. Over-the-air provisioning and set-and-forget lifecycle management make MobilePASS+ ideal for extending secure access to consultants, partners or a dispersed workforce.

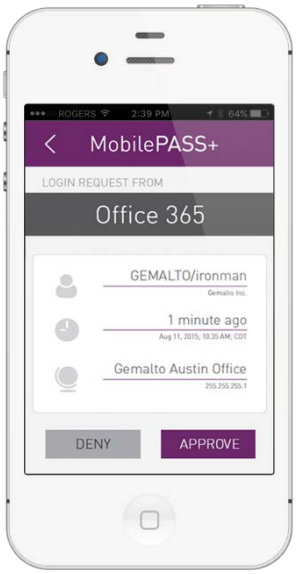

Figure 2: SafeNet MobilePASS+ next generation software token

IBM Multi-Factor Authentication for z/OS (IBM MFA for z/OS)

IBM MFA for z/OS provides a way to raise the assurance level of user authentication to z/OS applications and hosting environments by allowing the use of multiple authentication factors.

IBM MFA for z/OS helps protect corporations from these kinds of attacks by requiring the user to provide multiple pieces of evidence when they logon to prove that they are who they claim to be before being granted access. It uses a multitiered defense system to inhibit unauthenticated users from successfully accessing secured data or other assets. It combines several credentials: this can be something you know such as your Userid and Password, or a pin code; something you have such as a badge, or one-time password; or something you are (or something that is inherent) such as your fingerprint. With IBM MFA for z/OS, if one layer is compromised, other layers remain in place, presenting additional barriers to access. With the adoption of Multi-Factor Authentication, banks and financial institutions have increased confidence that only authorized users can access private, confidential data.

IBM MFA for z/OS is tightly integrated with z/OS Security Server (RACF®), which stores configuration and provisioning data, and provides an SMF audit trail to track authentication factors. IBM MFA for z/OS can also help provide security administrators with the ability to enforce a granular authentication policy on a per-user basis.

Regulations such as PCI DSS, NIST, and other regulations are driving the need for Multi-Factor Authentication as a requirement for compliance. IBM MFA for z/OS provides stronger, easier, authentication.

IBM Multi-Factor Authentication for z/OS and IBM RACF Integration

IBM MFA for z/OS and RACF are designed to enable multiple authentication factors that security administrators can utilize to enforce a granular multifactor authentication policy on a per-user-ID basis.

Applications can support IBM MFA for z/OS as part of their existing RACF authentication process. IBM MFA for z/OS is integrated with System Authorization Facility and the IBM RACF. When a user authenticates IBM MFA for z/OS with hard or soft tokens, the applicable Authentication Manager determines whether the user's credentials are valid. If they are, IBM MFA for z/OS then returns control to RACF to resume the authentication and authorization process. The solution is extensible, and as new authentication factors become available they can be added without requiring changes to the base infrastructure.

IBM MFA for z/OS support introduces extensions to a variety of components in RACF. For instance, it stores IBM MFA for z/OS fields in user and resource profiles managed by new RACF commands and callable services. The RACF database serves as the data repository for IBM MFA for z/OS data for auditing and reporting purposes. Simple user commands allow the provisioning and definition of the acceptable tokens for a user. Tokens can be specified during user authentication requests, enabling IBM MFA for z/OS aware applications to allow for factors in addition to RACF passwords. Auditing extensions track which factors were actually used during the authentication process.

Gemalto RADIUS Support in IBM MFA for z/OS

IBM delivered an IBM MFA for z/OS enhancement to support strong authentication to RADIUS-based integrations with Gemalto's SafeNet Authentication Service.

The token generated by the Gemalto's SafeNet Authentication Service can be used both in-band and out-of-band:

- In-band – By entering a password and a one-time passcode generated by SafeNet OTP 110, the user authenticates to the z/OS system.

- Out-of-band – After entering their username, the user receives an out-of-band push notification to their mobile device. The user taps to approve the login request and is then logged in to the z/OS system. A numeric or biometric PIN can be added for extra security.

Support for Gemalto's SafeNet Authentication Service is available with IBM APAR PI82734.

Protection Today and Tomorrow

IBM offers a highly flexible solution. Multiple authentication methods are supported which include one-time passcodes, out-of-band push authentication, context-based authentication and pattern-based authentication. Tight integration with RACF provides a consistent, policy-based, auditable approach.

IBM MFA for z/OS can help clients accelerate deployment, simplify management and more easily address regulatory compliance.

It can be used to secure mission-critical applications today as well as provide needed authentication to protect new mobile and cloud applications going forward.

IBM Corporation
New Orchard Road
Armonk, NY 10504

U.S.A.

Produced in the United States of America,
10/2017

ZSW03373-USEN-00