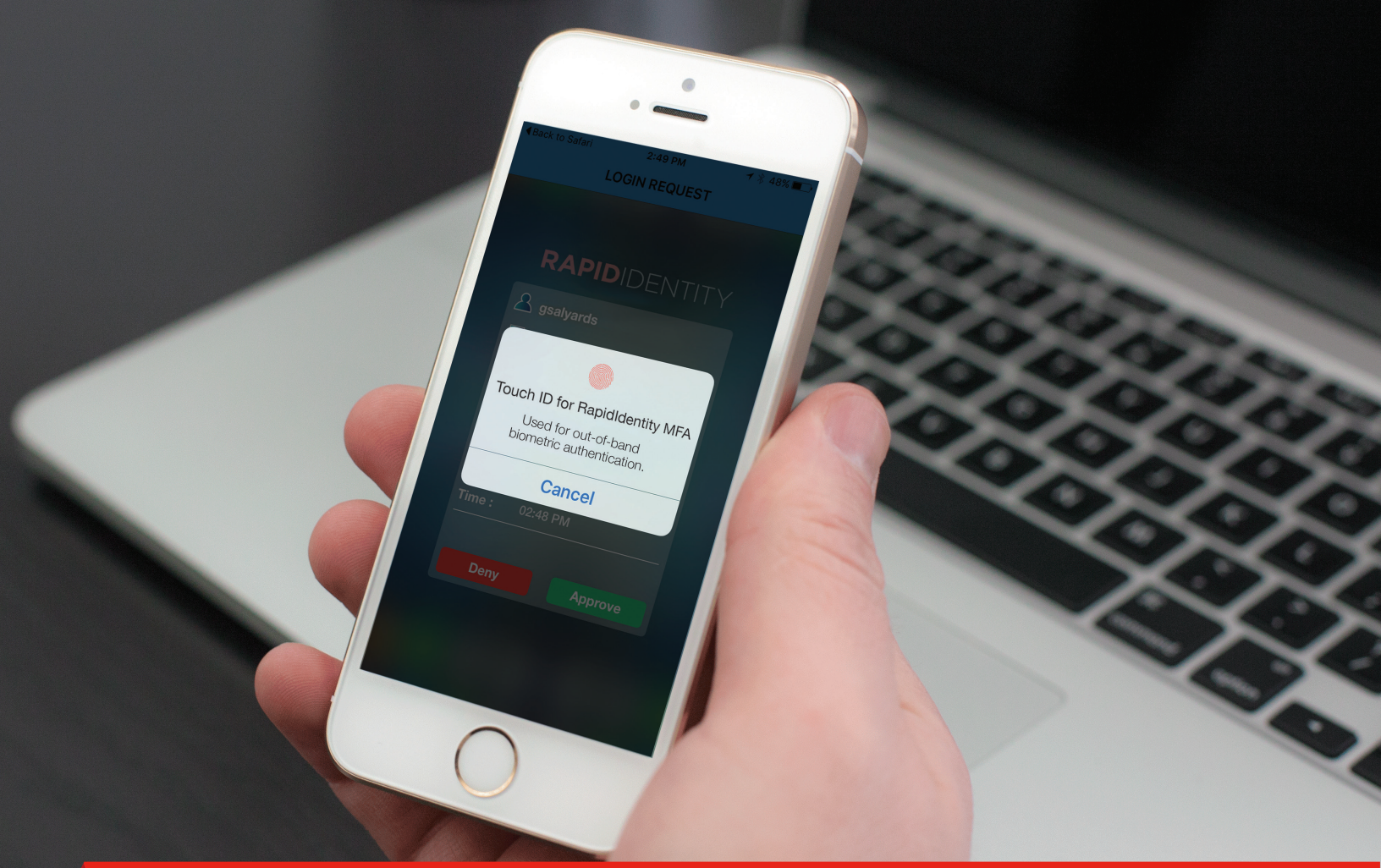

RAPIDIDENTITY MFA ONE TIME PASSWORD (OTP) SOLUTION BRIEF

IDENTITY AUTOMATION

OVERVIEW

RapidIdentity MFA enables OTP with tokens, cards, SMS, email, static TAN cards, voice, smart phones, and tablet applications that are available for free download from the Apple App Store, Google Play, and the Windows Phone Store.

The solution supports standard OTP and push notifications, with optional Apple TouchID support for logon to Windows, IPsec VPN, SSL-VPN, and a myriad of applications that support RADIUS or web-services. RapidIdentity MFA is based upon OATH's and HOTP event-based and TOTP time-based algorithms.

RapidIdentity MFA supports OTP devices from third-party vendors who support HOTP and TOTP, such as YubiKey™. This turn-key OTP solution includes the OTP device (physical or soft token) and the client software and management system, leveraging Microsoft's Network Policy Server (RADIUS). The solution is available on premises with a RapidIdentity Server or in the cloud with RapidIdentity MFA Cloud.

HOW DOES IT WORK?

An OTP is a password that is valid for only one login session or transaction and changes every 30 seconds.

OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into an application or to conduct a transaction will not be able to abuse the OTP, since it is no longer valid. OTPs are used commonly throughout the world for remote access. RapidIdentity OTP supports standard remote access requirements and adds push notification, Windows, and RapidIdentity MFA Shared Workstation logon capabilities.

RapidIdentity MFA manages the lifecycle of OTP token seeds that are assigned to users; the token seeds are then associated with the user and a specific device. The common workflow for OTP is for the user to enter a six digit code in conjunction with their username and an associated password or PIN. The codes can be entered into websites, VPNs, Windows, or with a RapidIdentity MFA Shared Workstation logon. The codes are generated on tokens or from within the RapidIdentity Mobile application. Once validated, the user is permitted access to the application, website, or desktop.

With RapidIdentity MFA PingMe, the user does not need to copy the OTP code, they simply enter their username and optional password or PIN into a website, VPN, Windows, or RapidIdentity MFA Shared Workstation logon. Once the username and optional password or PIN is verified, RapidIdentity MFA PingMe sends a push notification to the user's mobile device. The user reviews the information and chooses to approve or disapprove the request. RapidIdentity MFA PingMe is integrated with Apple TouchID for simple out-of-band biometric authentication.

RapidIdentity MFA Mobile OTP, enables companies to assign multiple user accounts to a single user's device. This gives users, such as administrators, the ability to log on to websites, applications, or desktops with the appropriate user account; thereby, addressing privileged access management concerns. RapidIdentity MFA Server manages the complete lifecycle of each user account.

HOW OTP WORKS WITH RAPIDIDENTITY MFA

HARDWARE TOKENS

The RapidIdentity MFA token is a time-based OATH compliant 6-digit LCD device. It is durable (lasting up to five years) and small, perfect for companies seeking the security of a hard token without the hefty price tag. It does not "expire," unlike other vendors' tokens.

INTEROPERABILITY

RapidIdentity MFA OTP works seamlessly with hundreds of leading applications from vendors and is tightly integrated into Windows for Windows logon, RapidIdentity MFA Shared Workstation login, and Microsoft RDP authentication.

Some of the apps we support are Cisco, Citrix, Dell, F5, Microsoft, NetMotion, Pulse Secure, and VMware.

EASE OF ADMINISTRATION

RapidIdentity MFA is specifically designed to be easy to use and manage. The browser-based application is deployed on IIS, integrates with Active Directory, and provides role-based access control for administration. Simplified deployment processes and polices make it easy for both small and large enterprises to deploy RapidIdentity MFA quickly.

Contact Sales: sales@identityautomation.com
Contact Support: support@identityautomation.com
Other information: info@identityautomation.com

Toll Free: 877-221-8401
Voice: 281-220-0021
Fax: 281-817-5579

Corporate Headquarters:
8833 N. Sam Houston Pkwy. W.
Houston, TX 77064