

# Frequently Asked Questions

## About Federal Zero-Trust Requirements and Defending Against Phishing Attacks

RSA is committed to supporting federal agencies and public sector organizations as they move to the cloud and work to meet new zero-trust directives. Part of that commitment is FedRAMP authorization of the RSA Cloud Services for government use.

RSA received FedRAMP Moderate Authorization designation through the JAB P-ATO process.

### What are the federal requirements for identity, multi-factor authentication, and zero trust?

Recently, the US Office of Management and Budget (OMB) released [Memorandum M-22-09](#) which requires agencies to achieve specific zero-trust security goals by the end of Fiscal Year 2024. Advancing toward zero trust is one of the main modernization goals for government cybersecurity as outlined in The [2021 Executive Order on Improving the Nation's Cybersecurity](#).

As described in the [Department of Defense Zero Trust Reference Architecture](#), "The foundational tenet of the zero-trust model is that no actor, system, network, or service operating outside or within the security perimeter is trusted." Instead, anything and everything attempting to establish access must be verified.

The move to zero trust emphasizes "stronger enterprise identity and access controls, including multi-factor authentication (MFA)" because without "secure, enterprise-managed identity systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks." The authentication processes must be able to "detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system." The memorandum also states that MFA should be integrated at the application layer, such as through an enterprise identity service, rather than through network authentication, such as a virtual private network (VPN).

## How does RSA support a zero-trust model and requirements?

RSA supports the move to a zero-trust model. We are helping organizations and agencies around the globe meet this new challenge through a complete and modern approach to identity and access management (IAM). RSA offers a range of MFA methods to meet the needs of different users and use cases. RSA re-establishes trusted user identities while simultaneously employing machine learning and risk-based analytics to detect anomalous activity including potential phishing attacks. We also offer intelligent governance and lifecycle capabilities that are designed to reduce an organization's attack surface. To protect the organization from both external and internal threats, our products eliminate over-entitlements that may be exploited by threat actors.

As we've helped our government agencies move toward zero trust and prepare for M-22-09 and the Executive Order, we've helped our customers answer a variety of questions about how to respond to these new requirements.

## What RSA solutions can help securely authenticate agency users?

RSA provides a broad range of strong MFA options to help Federal agencies securely authenticate users from anywhere to anything, including both next-generation and legacy agency systems. The move to the cloud, remote work, and digital initiatives have changed networks, and the perimeter that has historically protected resources continues to dissolve. Now people from every agency need to connect from many different locations; some even need to log in without internet access. This diversity of environments and users present a range of authentication challenges, yet government agencies need to be able to reliably deliver secure, convenient authentication no matter where people or devices may be located.

RSA solutions connect any user, from anywhere, to anything. We offer multiple authenticator choices to meet different agency requirements and user preferences, including support for FIDO. As a board member of the FIDO Alliance and co-chair of the Enterprise working group, we were pushing to remove passwords long before it was trendy, and we're glad some other [platforms](#) are now taking similar steps. Our identity platform supports [passwordless authentication](#) with 99.95% availability, including a no-fail capability that enables authentication without a network connection, so users can [authenticate securely even if connectivity is interrupted](#), or if they're without internet service.

## What authentication method is best to secure different types of applications?

RSA offers a variety of IAM capabilities to support the Federal requirements related to zero trust, cloud security, and authentication, and we are FedRAMP-authorized and trusted by the most sensitive government agencies. At this point, some agencies may have applications that don't support FIDO, and we are working to help customers as solution providers and companies transition their infrastructure and applications to support FIDO. RSA supports FIDO in our cloud solutions; our new DS100 authenticator is the market's first cloud-enabled, passwordless FIDO authenticator. In the meantime, agencies may continue to need one-time password (OTP) solutions, but it's important to realize that not all OTP solutions are created equal.

The securely implemented OTP used by RSA employs multiple controls to prevent an attacker from gaining access to a time-based OTP (TOTP). It also prevents the use of the TOTP in the rare instance an attacker does gain access. Unlike SMS TOTP, which has a time window that is typically 10-15 minutes, the RSA time window is only 60 seconds. Additionally, SMS OTP is transmitted over an insecure channel that is regularly a target of fraud abuse—TOTP isn't.

## How can OTP prevent a threat actor from gaining access?

Because the securely implemented OTP used by RSA limits the life of an OTP to just a minute, it prevents bad actors from storing authentication factors for later use. And even when a bad actor tries to reuse the OTP within that 60-second window, our authentication server will not accept an OTP it has already seen. This rejection creates an auditable event because the real user then must authenticate a second time to gain access, or the user is simply denied access. Only being able to use an OTP once to authenticate keeps a phisher from mirroring or storing a legitimate user's authentication attempt. Ensuring that OTP may only be used to authenticate once prevents a phisher from mirroring or storing a legitimate user's authentication attempt.

## How do RSA risk-based policies and identity governance enhance security?

The RSA machine-learning-based risk engine also detects behavioral anomalies. RSA risk-based authentication uses techniques and technologies to assess the risk an access request poses to the organization. Using machine-learning, the risk-based authentication learns from its assessments and applies that knowledge to future requests.

RSA not only secures authentication, but also the entire identity lifecycle with self-service password management, easy access certification, and automated joiner, mover, leaver (JML) processes, which ensure appropriate, compliant access throughout the user lifecycle. RSA manages the provisioning and deprovisioning of authenticators and provides help-desk tools to help handle situations like lost tokens and emergency access.

RSA also uses standards-based cryptographic methods to protect all the communication required to process an authentication attempt. We employ end-to-end encryption of both the PIN and OTP, which goes above and beyond transport layer encryption, so OTPs cannot be decrypted by a proxy. Our methods not only protect the OTP and PIN as they are transported in, out, and across networks but also ensure that the various software components can authenticate themselves.

## About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to [RSA.com](https://www.rsa.com).