RSA

CASE STUDY

Deploying Passwordless at One of the World's Largest Banks with RSA ID Plus

Cloud adoption lays the foundation for phishing-resistant passwordless authentication

In the security-first financial services sector, multi-factor authentication (MFA) has long been a linchpin of providing access that both maximizes security and minimizes inconvenience to users. Increasingly, forward-thinking banks are looking ahead to an authentication environment that still includes MFA—but also goes beyond it. Their vision is to achieve the goal of secure, convenient access by moving to passwordless authentication.

In that spirit, RSA is helping one of the largest banks in the world lay the foundation for realizing its vision of a fully passwordless future. The organization has adopted RSA® ID Plus, the complete, secure access management that provides a clear path to passwordless authentication, including phishing-resistant capabilities. The bank's goal in taking this step is to maximize security and convenience for internal users as well as contractors and customers.

RSA ID Plus: Building beyond MFA to a passwordless future

With the following unique combination of capabilities, RSA is well-positioned to help realize the bank's long-term vision of authentication without the risk and inconvenience that passwords impose.

- Provides a comprehensive platform for authentication in transition. As the bank evolves from on-premises to cloud authentication, RSA ID Plus smooths the transition by providing a full range of modern authentication capabilities to meet their needs at every point, with both MFA and passwordless methods, as well as a variety of phishing-resistant, FIDO2-certified hardware authenticators and software authenticators for passwordless environments.
- Addresses the needs of mobile and non-mobile users. ID Plus meets the authentication needs of all users whether they depend on mobile devices or on-premises methods to authenticate—or both. To implement passwordless securely, it's vital that banks and other organizations address all users, use cases, and environments, including internal users, external users like contractors and customers, and high-security environments.
- Works in cloud, hybrid, and on-premises environments. The bank can adopt ID Plus immediately, even while primarily providing on-premises capabilities to authenticate—and simultaneously move toward a hybrid or fully cloud-based deployment on its own terms and timeline. Using ID Plus provides the bank with hybrid failover capabilities for access and authentication, ensuring that users can still login securely even if they can't connect.

Customer Challenges

- Reducing the risk of data breaches associated with password-based access
- Adopting passwordless authentication that works well for all user populations
- Achieving phishing resistance

RSA Solution

- ID Plus cloud-based access management platform
- Broad range of passwordless authentication methods
- FIDO2-compliant authenticators, including device-bound passkeys

Goals

- Complete independence from password-based protection of secure resources
- Passwordless methods securing internal users, contractors, and customers
- Phishing-resistant authentication protecting all secure resources

RSA and FIDO2: Joining forces to deliver phishing-resistant passwordless authentication

The bank chose ID Plus as its SaaS solution with two primary goals in mind: conducting a broad passwordless initiative, and specifically adopting passwordless methods that provide anti-phishing capabilities. The FIDO2 open authentication standard for replacing passwords with stronger authentication methods is critical to meeting both of these goals.

RSA ID Plus provides FIDO2-based access through its Cloud Authentication Services (CAS) and FIDO2-certified authenticators. To resist phishing, **FIDO2 device-bound passkeys** are characterized by unique login credentials that are never stored on a server, as well as public-key cryptography that stores credentials in encrypted key combinations. FIDO2 also enables device-bound passkeys that never leave the user's device, further limiting phishing exposure.

RSA has a long history of collaboration and leadership with the **FIDO Alliance**, the industry consortium that developed the FIDO2 standard, and has been actively involved in developing and implementing FIDO2 and other FIDO technologies for reducing reliance on passwords.

FIDO2-certified authenticators: Delivering phishing-resistant passwordless authentication

RSA ID Plus supports phishing-resistant, passwordless authenticators, giving the bank a range of choices to meet its authentication needs for internal users, contractors, and customers. RSA phishing-resistant passwordless solutions include:

- ***RSA iShield Key 2 Series*** authenticators combine FIDO2, PIV, and HOTP and the FIPS 140-3 certified smart chip technology to provide the highest level of phishing-resistant, passwordless authentication.
- ***RSA Authenticator App*** device-bound passkeys are FIDO2-certified passwordless authentication methods stored only on a single device, which enhances security in general and phishing resistance in particular.
- ***RSA DS100 Authenticator*** is also designed for phishing resistance, offering MFA through both FIDO2 passwordless and OTP methods on a single cloud-enabled hardware token.

The goal: A phishing-resistant, fully passwordless environment

The bank is carrying out a long-term plan for meeting ambitious passwordless goals, with support from RSA at every step of the way, including on-site assistance from RSA Professional Services. The bank's goal is to completely remove the vulnerabilities associated with passwords and replace passwords with phishing-resistant, strong authentication for all secure resources, across a broad range of users—internal employees, contractors, and high-value customers. It's an ambitious project that will ultimately result in the realization of their vision of more secure, more convenient passwordless banking for all.

Learn more about how RSA supports banks and financial services.