RSA AUTHENTICATION MANAGER

Authenticators

AT A GLANCE

- The world's most popular and secure enterprise authenticator solutions
- Secures internal and remote network access
- Offers easy-to-use, "zero footprint" options
- Available in multiple form factors including hardware and software authenticators as well as Risk-Based and On-demand (SMS) authenticators

When organizations have confidence their information is secure, they are empowered to use it to accelerate their business. Identity assurance creates confidence and extends user authentication from a single security measure to a continual trust model that is the basis of how an identity is used and what it can do.

The RSA® Authentication Manager authenticators are a key component of an organization's identity assurance strategy. Trusted identities managed by RSA bring confidence to everyday transactions and support new business models providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience.

STRONG NETWORK SECURITY

Each RSA SecurID hardware or software authenticator has a unique symmetric key that is combined with a proven algorithm to generate a new one-time password (OTP) every 60 seconds. Patented technology synchronizes each authenticator with the security server, ensuring a high level of security. The one-time password—something the user has—is coupled with a secret personal identification number (PIN)—something the user knows—to create a combination that is nearly impossible for a hacker to guess. This protection is priceless when the risk of exposing critical information resources is considered.

HIGH QUALITY, RELIABLE AUTHENTICATION

For an enterprise depending on the broad distribution of authenticators to protect access to information and applications, token reliability is a major concern. RSA offers industry-leading levels of reliability and RSA SecurID hardware tokens are designed to withstand the worst imaginable conditions. From temperature cycling to mechanical shocks to being immersed in water, RSA SecurID hardware tokens are subjected to rigorous tests to ensure that user organizations do not face hidden costs due to token failures. By selecting RSA SecurID tokens, organizations can reduce the overhead costs of distributing replacement tokens and drive down the overall cost of security while providing a consistent and easy-to-use authentication experience for end-users.

CONVENIENT SOLUTION FOR END USERS

Whether hardware, software, Risk-Based or On-demand SMS, RSA authenticators are as simple to use as entering a password, but much more secure. For hardware and software tokens, ach end-user is assigned an authenticator that generates a one-time-use code. When logging on, the user simply enters this number plus a PIN to be successfully authenticated. For Risk-Based and On-demand (SMS) authenticators, convenient options for zero-footprint authenticators enable organizations the flexibility of extending applications to a greater population of users while at the same time maintaining the security posture of the organization.

A WIDE VARIETY OF AUTHENTICATON METHODS

One size does not fit all when it comes to choosing the right authenticator to balance your security, total cost of ownership and end-user security needs. With a broad range of easy-to-use form factors, there are RSA SecurID authenticators available to suit a wide variety of organization and application requirements. RSA offers hardware and software, as well as on-demand authenticators that provide strong authentication using familiar devices that users already have. RSA SecurID technology is also supported by a wide range of certified partner devices.

Hardware Authenticators

The RSA SecurID hardware token comes in a variety of convenient models that all generate and display new codes every 60 seconds.

RSA SecurID 200

The RSA SecurID 200 is the original RSA SecurID hardware token. This business card holder-sized device provides the same excellent performance guaranteed from every RSA SecurID authenticator.

RSA SecurID 520

The RSA SecurID 520 PINpad model is the same size as the RSA SecurID 200 but has a PINpad feature that enables users to encrypt their passcode for a higher level of security.

RSA SecurID 700

The RSA SecurID 700 is a small key fob that connects easily to any key ring and fits into a user's pocket or small carrying case.

RSA SecurID 800

The RSA SecurID 800 offers the one-time password functionality of the other hardware authenticators and can be used for storage of Windows® username/password credentials and digital certificates—creating a master key for multiple authentication methods. When connected, the RSA SecurID 800 is enabled for automatic token code entry, allowing applications to programmatically access token codes directly off the device and eliminating the need for the user to type their code.

SOFTWARE AUTHENTICATORS

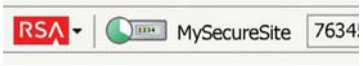
RSA SecurID software tokens use the same algorithm as RSA SecurID hardware tokens while eliminating the need for users to carry dedicated hardware devices. Instead of being stored in hardware, the symmetric key is safeguarded securely on the user's PC, smart phone or USB device. RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. Software tokens can help the enterprise cost-effectively manage secure access to information and streamline the workflow for distributing and managing two-factor authentication for a global work force. Additionally, software tokens can be revoked and recovered when someone leaves the company or loses a device, eliminating the need to replace tokens.

RSA SecurID software tokens are available for a variety of smart phone platforms including BlackBerry™, iOS, Android, and Microsoft Windows Phone.

RSA SecurID Token for Windows and RSA SecurID Token for Mac OSX

The RSA SecurID Token for Windows and RSA SecurID Token for Mac OSX are convenient form factors that reside on a PC or Mac and enable automatic integration with leading remote access clients. An extra layer of security can also be added to the RSA SecurID Token for Windows when it is used in conjunction with the Dell® E-family of Latitudes, where the token can be embedded in a secure chipset.

RSA SecurID Toolbar Token



The RSA SecurID Toolbar Token combines the convenience of auto-fill capabilities for web applications with the security of anti-phishing mechanisms.

RISK-BASED AUTHENTICATION AND ON-DEMAND

Risk-Based Authentication is a multi-factor authentication solution that strengthens traditional password-based systems by transparently assigning a risk level to each login request. A powerful risk engine evaluates each attempted login and activity in real time by tracking hundreds of risk indicators and determining the risk associated with each access request.

Risk-Based Authentication enables organizations to extend secure remote access privileges to a diverse user base and access points – both internal and external – without having to compromise on user convenience or privacy.

RSA Authentication Manager 8.x enables Risk-Based Authentication to be deployed on a single platform alongside RSA SecurID hardware and software authenticators. Balance security, cost, and convenience to achieve strong authentication that protects a wide range of users and use cases.

The RSA On-demand Authenticator is an innovative solution that enables users to receive a one-time password as an SMS message delivered to their cell phone or via e-mail. Users are sent a one-time password to use as a login to their SMS-enabled mobile device. The On-demand Authenticator is a true zero footprint authenticator and requires no hardware or software token to be deployed.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

RSA STORE: CONFIGURE AND COMPARE

Compare features, see options, and get pricing for RSA SecurID. Visit the RSA Store now.

RSA

EMC²