



The Security Division of EMC

RSA Solution Brief

RSA® SecurID Two-factor Authentication



Today, we live in an era where data is the lifeblood of a company. Now, security risks are more pressing as attackers have broadened their targets beyond financial information and personal identities. They are becoming increasingly daring and manipulative as they target intellectual property and trade secrets making information systems that rely on static passwords more vulnerable and at risk than ever. The cause for concern is only magnified as the cost associated with a data breach has reached an estimate of \$ 6.6 million¹.

Additionally, government regulations such as Sarbanes-Oxley, PCI Data Security Standard, US Data Breach Notification Laws and others have been put in place to protect access to corporate networks. Failure to meet requirements that call for the implementation of two-factor authentication could result in regulatory fines and irreversible damage to a brand's reputation.

Whether it is avoiding data breaches, decreasing costs or complying with government regulations, protecting access to critical information with a strong two-factor authentication solution is a necessary component of any organization's overall strategy.

RSA SecurID Two-Factor Authentication

As the market-leading two-factor authentication solution, RSA SecurID offers the strength of security, broad application support, variety of authentication methods and reliability required to protect the network assets of companies worldwide. The components of this solution include RSA Authentication Manager software, RSA Authentication Agents, and RSA SecurID authenticators.

Each RSA SecurID 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 Authentication Manager server, ensuring a high level of security. The one-time password – something you have – is coupled with a secret personal identification number (PIN) – something you know – to create a combination that is nearly impossible for a hacker to guess. RSA SecurID authentication provides anytime, anywhere, secure access to VPNs, wireless access points, web applications and network operating systems and more.

RSA Authentication Manager, RSA SecurID Appliance, & RSA Authentication Agents – Security, Scalability and Interoperability

RSA Authentication Manager

RSA Authentication Manager software is the management component and engine behind the RSA SecurID industry-leading two-factor user authentication technology. It is used by more than 30 million end-users worldwide to verify authentication requests and centrally administer user authentication policies for access to enterprise resources. Designed to fit the needs of organizations of all sizes, RSA Authentication Manager software is built upon an enterprise class multi-processor architecture that is capable of handling from as few as twenty-five users to millions of users per server and hundreds of simultaneous authentications per second.

RSA Authentication Manager software offers high performance and scalability with enterprise-level management features such as database replication, logging and reporting, native LDAP support, and web-based management. The database replication feature enables flexible network configuration and load balancing for improved performance that ultimately

¹ Ponemon Institute 2008 Annual Study, " *Cost of a Data Breach* "



lowers management costs. Administrators are able to use RSA Authentication Manager as an auditing, accounting, and compliance tool as it logs all transactions and user activity. In addition, report templates are available that can be easily tailored to administration needs, including activity, exception, incident and usage summaries. Delivering true native LDAP support for direct integration with Sun One and Microsoft Active Directory, the RSA Authentication Manager software requires no synchronization. The browser-based administration interface of RSA Authentication Manager calls for no client software installation, and can be remotely administered from any PC with a browser and Internet connection.

RSA Credential Manager is tightly coupled with the management interface of RSA Authentication Manager, and requires no separate install. It offers functionality such as self service, allowing end users to request a variety of services such as on-demand token codes for emergency access, and workflow provisioning, allowing administrators to create processes by which requestors are approved and credential are issued.

RSA Authentication Manager is interoperable with many of the major network infrastructure and operating system products on the market, including more than 400 products from over 200 vendors, providing organizations with maximum flexibility and investment protection.

RSA SecurID Appliance

The RSA SecurID Appliance delivers RSA Authentication Manager in an integrated, rack-mountable hardware appliance. It is easy to deploy and maintain, and designed so that a customer can be up and running in as few as 30 minutes.

The RSA SecurID Appliance is a flexible and scalable solution that is available in two models that can be configured to meet the different needs of organizations of any size.

RSA SecurID Appliance 130

The RSA SecurID Appliance 130 is designed to satisfy the requirements for simple, cost-effective deployments

RSA SecurID Appliance 250

The RSA SecurID Appliance 250 is designed with dual power and redundant discs for organizations that require high availability (HA) deployments.

RSA Authentication Agents

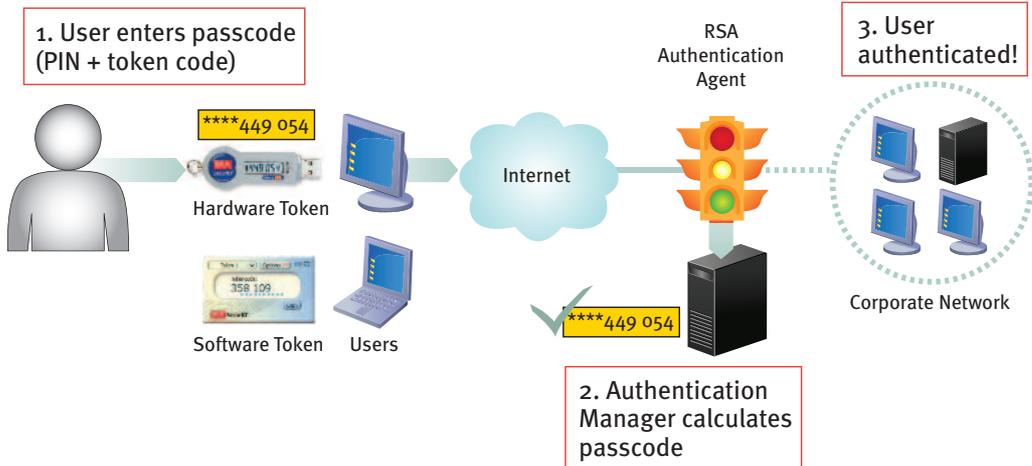
RSA Authentication Agent software functions much like security guards, standing between the user and a protected resource or device to enforce two-factor authentication via the RSA Authentication Manager software. Agents provide load balancing by detecting replica server response times and responding accordingly

RSA Authentication Agent software is embedded in Remote Access Servers (RAS), firewalls and Virtual Private Networks (VPNs), virtually ensuring that RSA SecurID technology will work seamlessly in any customer environment.

In addition, agents let you secure web pages and applications on your intranet or extranet, at the same time protecting mission-critical back-end systems. Agents are also available to provide secure access to NT domains and resources hosted on UNIX servers, mainframes, mid-range systems and a range of legacy hosts. Software toolkits make it possible to create custom agents to protect other internal applications that are specific to a particular organization.



How Does RSA SecurID Work?



Step 1: When the user attempts to access a protected resource, like a VPN or secure portal, they are prompted for their user ID and passcode. The passcode that the user presents is a combination of their secret PIN and the OTP code that is displayed on their token at that moment in time.

Step 2: The user ID and passcode are intercepted by the RSA Authentication Agent and presented to the RSA Authentication Manager software, the system's authentication engine. The software checks the passcode to ensure it is correct before issuing instructions to the system to either allow or deny access.

Step 3: Once access is allowed, the user is authenticated and has access to their network resources.

RSA SecurID Authenticators – Quality, Reliability and Choice

One-size does not fit all when it comes to choosing the right authenticator to balance your organization's 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 requires.

RSA SecurID Hardware Tokens

RSA SecurID hardware tokens are designed to withstand the worst imaginable conditions to ensure that you do not face hidden costs due to token failures. By selecting RSA SecurID tokens, which come with a lifetime warranty, 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.

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



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 RSA SecurID hardware, the symmetric key is safeguarded securely on the user's PC or smart phone. RSA SecurID software authenticators help to more effectively manage cost while reducing the number of items needed to gain access to the network or corporate assets, and eliminating the need for replacement tokens in the event of someone leaving the company or losing a token.

RSA SecurID software tokens for smart phones



RSA SecurID software tokens are available for a variety of smart phone platforms including BlackBerry®, iPhone®, Windows® Mobile, Java™ME, Palm OS and Symbian OS

and UIQ devices. Integrating the RSA SecurID token on the smart phone makes it easy for your employees to remember and use.

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 resides on your PC or Mac and enable automatic integration with leading remote access clients.

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.

RSA SecurID On-demand Authenticator



The RSA SecurID On-demand Authenticator enables users to receive a one-time password as an SMS message delivered to their

cell phone or via e-mail. Users request a one-time password through an intuitive self service web module by entering their PIN. The On-demand Authenticator is a true zero footprint authenticator and requires no hardware or software token. It's a great choice for users that do not need to frequently access the network remotely.

RSA Secured Partners – Turnkey Interoperability

Ensuring that RSA SecurID integrates easily into your existing infrastructure is a top priority for RSA. The RSA Secured Partner Program works with leading vendors of remote access products, VPNs, firewalls, wireless network devices, web servers and business applications to certify product integrations with



RSA Authentication Manager, providing customers with faster time to deployment and lower overall ownership costs. With built-in interoperability with more than 400 certified products from over 200 vendors, RSA SecurID two-factor authentication provides organizations with maximum flexibility and investment protection. For more information about our partners, visit www.rsasecured.com.



About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used. RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2010 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, the RSA logo and SecurID are trademarks or registered trademarks of RSA Security in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and/or services are trademarks of their respective companies.
SIDTFA SB 0210

Why RSA SecurID?

RSA SecurID provides customers with the most secure, high-quality, cost-effective two-factor authentication solutions that meets the needs of customers of all sizes. The five key attributes are:

Strength of Security

- The RSA time-synchronous solution combined with the AES algorithm with which our tokens are built, provides a higher level of security than many alternatives.
- RSA Labs continues to advise the product team of all new threats so we can constantly improve our offering.

Broad Application Support

- RSA has the largest number of integration partners, offering guaranteed RSA SecurID interoperability with more than 400 applications. This ensures that the RSA SecurID will work within your current infrastructure with no hidden costs.

Breadth of Offering

- RSA offers a wide range of options to meet current and future needs of organizations – hardware tokens, hybrid authenticators, software tokens, SMS, Adaptive Authentication.
- Authentication Manager can be delivered in a variety of ways to fit in to the customer's IT environment – Appliance, Software, SaaS.

Quality and Dependability

- Authentication Manager includes redundancy, failover and other mission critical features, ensuring it will always be running whenever your users need it.
- All hardware tokens have lifetime warranties and are most reliable in industry, saving organizations time and money for not having to redeploy when tokens are damaged.

