

The Power Behind RSA SecurID® Two-factor User Authentication: RSA® Authentication Manager

Information security is a necessary underpinning for further advances in electronic business. Technologies such as session encryption, firewalls, virtual private networks, wireless LANs and digital certificates have all emerged as pieces of the solution. While each is designed to enhance some aspect of information security—whether by restricting access to or preventing the interception of private data—none of them alone is designed to address the fundamental security issue that underlies the most damaging information crimes such as “is the person who is attempting to access protected files and/or resources an authentic user or an impostor?”

This white paper discusses how RSA Authentication Manager software, as an integral component of the RSA SecurID® solution for two-factor user authentication, can help efficiently manage the authentication of users to your network, Web-based applications or applications within your network. The key security, operational and market issues that are relevant to this discussion are also examined.



Confidence Inspired™

TABLE OF CONTENTS

I. USER AUTHENTICATION: AN E-BUSINESS ENABLER	1
II. THE RSA SECURID SOLUTION FOR TWO-FACTOR USER AUTHENTICATION	2
III. KEY BENEFITS OF RSA AUTHENTICATION MANAGER AND RSA SECURID	4
IV. PREVENTING UNAUTHORIZED ACCESS WITH RSA AUTHENTICATION MANAGER AUTHENTICATION	6
V. FUNCTIONAL DETAIL	8
VI. RSA AUTHENTICATION MANAGER ADMINISTRATION	10
VII. RSA AUTHENTICATION MANAGER ENTERPRISE EDITION LICENSE	12
VIII. CONCLUSION	13
IX. ABOUT RSA SECURITY	14

**I. USER AUTHENTICATION:
AN E-BUSINESS ENABLER**

User authentication is an e-business enabler.

If you can trust the identity of the employee who is attempting to connect to your corporate network from home, while traveling or when roaming within the complex using the corporate wireless network, you can improve his productivity and facilitate your business by giving him access to the data he needs.

If you can trust the identity of the resellers who are attempting to access your partner web portal, you can make available, on that portal, key information which will help them make a sale without worry that you will be exposing such information to a competitor or customer.

If you can trust the identity of customers who are attempting to access your web-based knowledge database, you can serve them better by providing them with up-to-date information while saving support costs.

An authentication server is no longer a tactical point solution for one group or a single application. Rather, authentication servers such as the RSA Authentication Manager solution have become a mission-critical, strategic component of the network infrastructure. As employees and strategic partners increasingly decide to log in from home or need to log in from remote offices, the need for a

security solution that is robust and easy to administer becomes critical. Customers will need access to your extranet or intranet and the security administrator will need to be able to quickly administer their security privileges—before they are lost as customers. It is vital, therefore, to have a fast, scalable and efficient authentication solution.

User authentication also prevents fraud.

Many of the most damaging crimes online have a common denominator: the circumvention of password protection to gain access to information or funds. While basic passwords may be sufficient to safeguard non-critical systems, an organization’s sensitive applications, files and systems demand a higher order of protection. Fortunately, a single security approach can be used to deal with the entire spectrum of intrusions that result from password breaches: replacing basic password security with a two-factor user authentication solution. This solution not only mitigates the risk of security breaches but also enables companies to comply with customers and strategic partners who demand secure e-commerce, thereby avoiding the long-term costs associated with security breaches and helping to increase revenues.

What Value/ROI?	Which Solution?	Which Vendor?
<ul style="list-style-type: none"> • New revenue streams • New customers • New markets • Competitive advantage • etc. <p style="text-align: right;">HIGHER REVENUES</p>	<ul style="list-style-type: none"> • Acquisition • Deployment • Operating <p style="text-align: right;">TOTAL COST OF OWNERSHIP</p>	<ul style="list-style-type: none"> • Total cost of ownership • Technical architecture • Vision • Financial viability • Trustworthiness • Service & support <p style="text-align: right;">VENDOR SELECTION CRITERIA</p>
<ul style="list-style-type: none"> • Cost reduction • Cost avoidance • Efficiency • Effectiveness <p style="text-align: right;">LOWER COSTS</p>	<ul style="list-style-type: none"> • Convenience / ease of use • Portability • Multi-purpose <p style="text-align: right;">STRATEGIC FIT (USERS)</p>	<p>When evaluating an authentication solution the following questions must be asked:</p> <ul style="list-style-type: none"> • What is the value of the solution? What return on investment (ROI) will it bring? (Section III) • Which authentication solution is the best fit for your organization? (Sections IV-VII) The answer to this question depends on more than relative security and acquisition cost and includes factors such as convenience for end users, interoperability and future flexibility. • Which vendor is the best partner for providing such a solution? (section IX)
<ul style="list-style-type: none"> • Regulations • Customers • Partners • Competitors • Internal <p style="text-align: right;">INCREASED COMPLIANCE</p>	<ul style="list-style-type: none"> • Relative Security • Interoperability / back-end integration • Robustness / scale • Future flexibility <p style="text-align: right;">STRATEGIC FIT (CORPORATE/SYSTEM)</p>	
<ul style="list-style-type: none"> • High value information • High value transactions <p style="text-align: right;">MITIGATED RISK</p>		

II. THE RSA SECURID® SOLUTION FOR TWO-FACTOR USER AUTHENTICATION

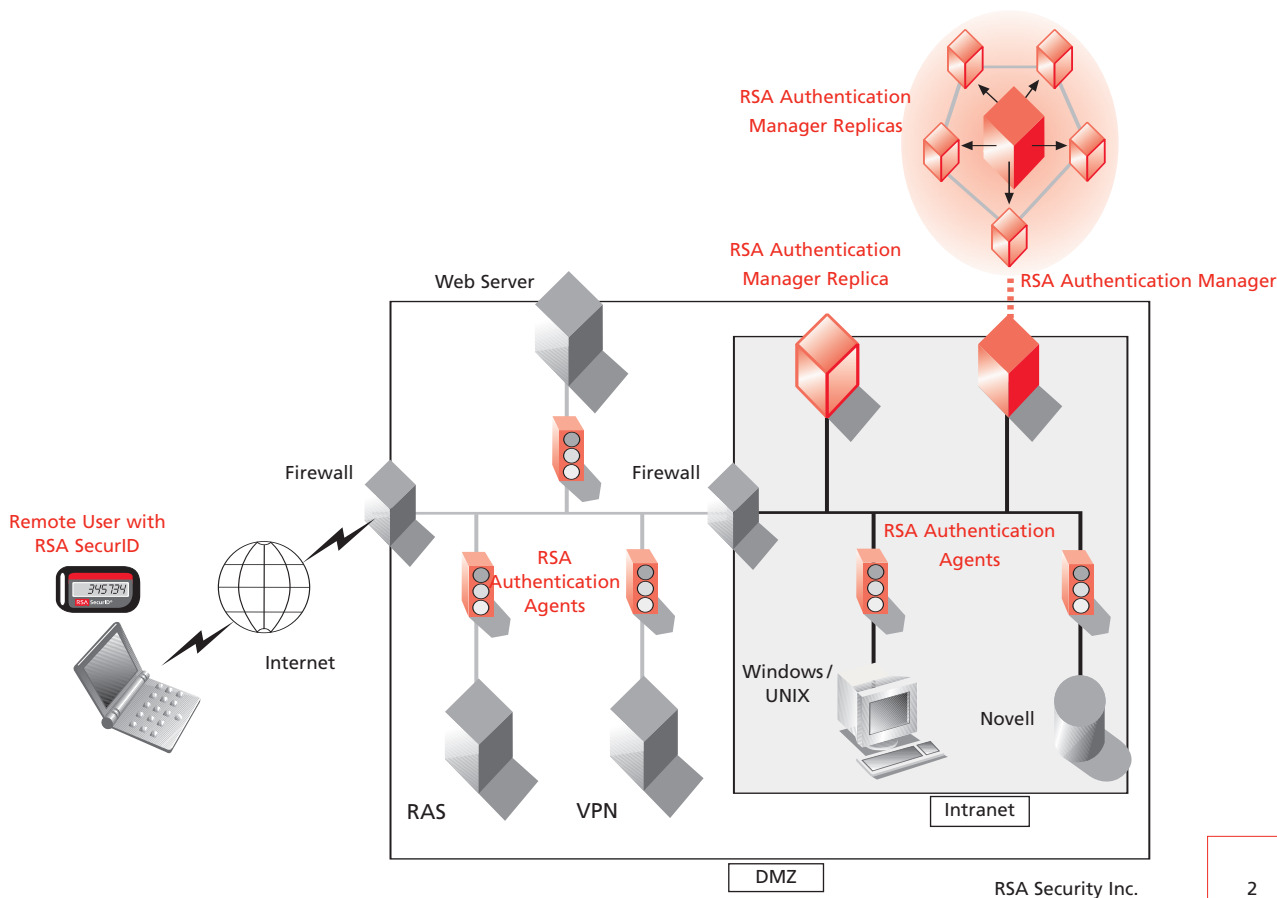
The RSA SecurID® solution for user authentication is built on an approach called “two-factor authentication.” The premise of this approach is that a single, remembered factor such as a password inherently provides a low proof of authenticity, since anyone who overhears or steals the password will appear completely genuine. It is the addition of a second, physical proof that makes the certainty of authenticity exponentially higher. The bank ATM card is an example of a widely used form of two-factor authentication; requiring the combination of a PIN and also a valid ATM card provides a sufficient level of security to support access to bank services and funds.

With the RSA Security solution for two-factor user authentication, authorized users are issued individually registered RSA SecurID tokens that generate single-use token codes, which change based on a time code algorithm. A different token code is generated every 60 seconds. The authentication server (RSA Authentication Manager) that protects the network and e-business applications validates this dynamic code. Each RSA SecurID token is unique and it is impossible to predict the value of a future token code by recording prior token codes. Thus when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is the valid user in possession of the RSA SecurID authenticator.

Working Together: Server, Client and Intermediary Agent

User authentication for wired or wireless local network access, remote dial-in, Internet/VPN connections or web applications is accomplished via the RSA Authentication Manager authentication server. When a user attempts to access a protected system, a special software agent—called an RSA Authentication Agent—initiates an RSA Authentication Manager authentication session instead of a basic password session. Most leading remote access server, firewall, VPN, wireless access and router products have built-in RSA Authentication Agents for out-of-the-box compatibility with RSA SecurID two-factor authentication. In addition, both TACACS+ and RADIUS authentication sessions are supported by the RSA Authentication Manager software. RSA Authentication Manager software includes a RADIUS server, so companies can manage user accounts from a single database for both RADIUS and RSA SecurID authentication.

In a two-factor authentication session, the user is required to enter a user name and—in lieu of a password—a PIN number plus the current token code from his or her RSA SecurID authentication device. The agent transmits the information to the RSA Authentication Manager software, which approves access when the information is validated. The user is granted access appropriate to his or her authorization level, which is noted by the RSA Authentication Manager software in its log file.



RSA Authentication Agents

Web Access

- Microsoft IIS
- Apache
- Stronghold
- SunONE

Local and Remote Access

- Windows 2000, 2003
- Windows XP
- Solaris
- IBM AIX
- HP-UX
- Red Hat Linux
- NMAS (Novell Modular Authentication System)

For more detailed information on RSA Authentication Agent support go to <http://www.rsasecurity.com/products/secuid/authenticationagents.html>

RSA SecurID Authenticators

Secure network access and access to e-business applications begins with ensuring that users are strongly authenticated using an RSA SecurID authenticator. RSA SecurID authenticators are offered in many forms: hardware tokens, software tokens, smart cards and USB devices. The most common hardware form is the key fob, a device with a built-in chip, an LCD window capable of displaying up to an eight-digit number (or token code), yet small enough to be attached to a key ring. When shipped from RSA Security, the key fob is initialized with a unique seed value; each minute, the internal chip performs an algorithm combining and scrambling the seed value and current time, to create a pseudo random number.

In addition to the key fob style, other token types include a credit card-sized authenticator and the RSA SecurID PINPAD technology model, which requires the entry of the user's PIN in order to display the token code, and the RSA SecurID Software Token for Windows desktops, the Palm™ Computing Platform, Microsoft® PocketPC devices, BlackBerry handhelds and cell phones, which duplicates the function of the RSA SecurID PINPAD token in the form of a software utility. The RSA SecurID Software Token seed value can also be stored on the RSA SecurID Smart Card or USB Token. The RSA SecurID Software Token technology is copy-protected to prevent duplication from machine to machine.

All RSA SecurID authenticators operate using the same patented technology to generate the pseudo-random token code. RSA SecurID authenticators have been designed to take advantage of the industry standard AES algorithm. Our customers enjoy the benefits of integrity and assurance of quality that is provided by using the industry standard AES algorithm.

RSA Authentication Agents

The intermediaries that enable this two-factor authentication are implementations of RSA Authentication Agent technology, which functions much like a security guard, enforcing security policy as established within the RSA SecurID system. RSA Authentication Agent technology is built into most leading network equipment, as well as software systems (a complete list of companies that support two-factor authentication via built-in RSA Authentication Agent technology is available at www.rsasecured.com). In addition, RSA Security offers RSA Authentication Agent software to provide strong authentication to popular web servers (such as Microsoft® IIS, Apache and SunONE*) as well as RSA Authentication Agent software to help to protect UNIX environments.

A Unique Solution for Microsoft® Windows® Operating Environments

When used in conjunction with RSA Authentication Agent for Microsoft® Windows® software, the RSA Authentication Manager is an ideal solution for organizations seeking strong user authentication to Microsoft operating environments. Using innovative new technology, the RSA SecurID for Microsoft Windows solution allows RSA SecurID authentication to a Microsoft environment whether the user is online or offline. The solution strengthens security in a Windows environment, and provides a simple and consistent method for user authentication.

RSA Authentication Manager software supports RADIUS authentication; using the RSA Authentication Manager, all RADIUS users and clients can be managed centrally. RSA Authentication Manager software also supports the TACACS+ authentication protocol.

Most RSA Authentication Agent software uses 128-bit RC5® to encrypt the communication to the RSA Authentication Manager software. Some implementations of the RSA Authentication Agent software also use SHA-1 or a proprietary hashing algorithm to hide the user's PIN and token code inside the encrypted packet.

A single RSA Authentication Manager instance can support thousands of RSA Authentication Agent implementations, offering broad capacity to protect enterprise resources.

*Lotus Domino support is available through Winchester Business Systems, Inc.

Administration of RSA Authentication Agent software and setting of policies is done centrally via a Windows based admin application that allows security managers to select and apply settings to users and protected resources by pointing and clicking rather than writing custom code. A client auto-registration feature automates the task of creating and updating settings securely at each RSA Authentication Agent implementation.

RSA Authentication Manager

In the RSA SecurID solution, the authentication engine on the network is the RSA Authentication Manager software. Managed by the security administrator or network manager, RSA Authentication Manager software is used to help:

- Assign RSA SecurID authenticators to trusted individuals
- Set and enforce security policies, protecting access to private network systems, files and applications. This includes the ability to define access based on time of day, day of week or by group or user-defined access
- Maintain audit logs of user access and administrator activity
- Centrally manage user, group, agent, Replica and token information

RSA Authentication Manager software operates on Windows and UNIX-based server platforms. A single RSA Authentication Manager implementation can authenticate over a million users.

Database Replication is an important feature for companies that need high performance to support large user bases and the convenience of administering user authentication across the network. This level of redundancy not only provides 24/7 availability, but also allows customers to plan efficient, economic global network topologies.

RSA Authentication Manager software has a number of advanced administrative and security monitoring capabilities (discussed later in this document), including the ability to delegate various levels of management tasks, centrally manage user and token information and perform system management remotely from a Windows desktop or web browser.

An RSA ACE Server Base license allows for 2 simultaneously authenticating servers: 1 Primary and 1 Replica server. An RSA Authentication Manager Advanced license allows for 1 Primary and as many as 10 Replica servers to interoperate within one realm and up to 6 realms to be networked together. The benefits of RSA Authentication Manager Advanced licenses are discussed in more detail later in this document.

RSA Authentication Deployment Manager

A web-based workflow system, RSA Authentication Deployment Manager software helps reduce administrative costs by offering end users a self-service platform to request, activate and initiate deployment of RSA SecurID credentials. The system automates the entire credential deployment process—including populating RSA Authentication Manager with user data, token assignment and activation, and facilitation of the fulfillment of RSA SecurID token requests. Flexible and scalable, RSA Authentication Deployment Manager is ideal for both enterprise and e-business related deployments, making issuing credentials faster, more efficient and easier than ever.

RSA Authentication Deployment Manager is included with an RSA Authentication Manager Enterprise Edition license and available at additional cost with an RSA Authentication Manager Base Edition license.

III. KEY BENEFITS OF RSA AUTHENTICATION MANAGER AND RSA SECURID

RSA Authentication Manager software offers a superior return on investment for enterprises by helping to enable revenue-generating processes, lower costs, ensure compliance and mitigate risk.

Revenue Generation

By providing the ability to strongly authenticate users and establish trust, the RSA SecurID solution allows enterprises to confidently automate and web-enable their critical business processes and thereby reach new customers and new revenue streams. The RSA SecurID solution helps enable enterprises to make critical information available online or through a VPN or remote access server which in turn enables employees and strategic partner to access and use that information to provide services and close deals.

The broad interoperability of the RSA SecurID solution gives customers the flexibility to efficiently protect incremental applications with RSA SecurID technology bringing greater trust in end user identity and higher security to additional applications.

Cost Savings

The RSA SecurID solution can save enterprises money by replacing password systems. Password systems are expensive to maintain due to the hidden costs associated with help desk calls and lost user productivity. The RSA SecurID solution reduces these costs significantly by reducing the number of passwords required for each user and simplifying the authentication logon process.

The RSA SecurID solution is easy for end users to use. Because of its simple, straight-forward approach, end users are quick to embrace and use the system. The breadth of choice in authenticator form factors (from hardware tokens that can be kept on a key chain to software tokens that run on a PDA or desktop) ensures it will fit most customer situations.

RSA Authentication Manager software is easy to install and deploy. Token deployment is further facilitated by RSA Authentication Deployment Manager, a provisioning application, which can greatly speed the rollout and reduce costs of RSA SecurID authenticators to end-users.

Through the RSA SecurID Ready program, the RSA Authentication Manager technology is instantly compatible with the industry's leading security and networking products. Over 185 companies have developed over 270 products that are designed to work seamlessly with the RSA SecurID solution. This out-of-the-box interoperability can significantly reduce integration costs and safeguard existing investments. For a complete list of RSA SecurID Ready strategic partner and hands-on Implementation Guides, refer to www.rsasecurity.com/partners/secured/securidpartners.html.

RSA Authentication Manager software lowers administration costs by allowing for centralized user management, a hierarchy of administration through administrator scoping and task lists and web-based administration for help desk administrators. An LDAP synchronization utility enables centralized administration of user information in an LDAP directory. User information can be synchronized automatically from the LDAP directory into RSA Authentication Manager technology according to schedulable synchronization jobs.

With database replication, companies can track user authentication to their network anywhere in the world in real time, update security policy simultaneously across their worldwide networks and develop a global network topology that increases the performance of their network. RSA Authentication Manager software enables companies to accomplish all of this by providing flexible network configuration, load balancing and, ultimately, simplified and lower cost of management.

Compliance

RSA SecurID technology can help enterprises meet their industry compliance requirements and governmental regulations by ensuring the authenticity of users accessing sensitive information. Strong two-factor authentication, like that provided by RSA SecurID technology, can assist enterprises in complying with regulations in the United States such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in health care, the Gramm-Leach-Bliley Act (GLB Act) in Financial Services and European regulations such as the e-signature laws.

In addition, some companies may require their suppliers and strategic partner to have adequate security, including two-factor authentication, in place.

Mitigated Risk

RSA Authentication Manager software helps reduce the risk of authentication downtime. It is a robust, highly available solution, capable of handling millions of users and hundreds of simultaneous authentications per seconds. Support for a Primary server and up to 10 Replica servers per realm provides automatic load balancing and fail over to increase performance and scalability for authentication to a variety of applications, including VPN, RAS, Wireless LAN, Windows and web.

If the Primary server fails, disaster recovery functionality enables the rapid promotion of a Replica server to be the new Primary server—quickly restoring administration of the realm.

RSA SecurID technology helps reduce the risk of security breaches thereby saving the customer money, time and the embarrassment of negative publicity. RSA Authentication Manager software offers superior security. Based on RSA Security's technology and expertise in encryption, the RSA Authentication Manager technology's implementation is highly secure. RSA SecurID technology uses a patented, time synchronous, two-factor authentication mechanism to validate users.

RSA Authentication Manager software is a well-tested, production-proven product that has been designed to meet the requirements of the most demanding environments. With over 15,000 customers and more than 14,000,000 users testing the limits of the system daily, RSA Authentication Manager software is an award-winning, market-leading, well-proven solution.

IV. PREVENTING UNAUTHORIZED ACCESS WITH RSA AUTHENTICATION MANAGER AUTHENTICATION

Additional benefits of using RSA Authentication Manager software to prevent unauthorized access to enterprise networks or specific applications include:

Enterprise Authentication

RSA Authentication Manager software limits access only to those users who provide a valid PIN/token code combination; this gives organizations a very high assurance that those persons logging on are, in fact, the authorized individuals, vastly reducing the risk of attacks or unauthorized access. Even enterprise networks with millions of users and multiple worldwide offices can be protected, with database replication and cross-realm features to seamlessly support authentication of users traveling outside of their home realm.

Access Control

The RSA Authentication Manager technology lets organizations deploy RSA Authentication Agent software to protect various access ports, as well as data files, applications and other resources. By grouping users in the RSA Authentication Manager database, organizations can easily and centrally designate access to certain resources. Customers may also choose to deploy RSA Authentication Manager software together with RSA Access Manager software to enable more granular web access management.

Evasion of Attack

RSA Authentication Manager software will automatically disable a token after a series of failed attempts, such as a series of incorrect PINs or token codes. Hackers will try unexpected means to gain access to an enterprise network or a specific e-business application on that network. By monitoring the RSA Authentication Manager logs or events which the RSA Authentication Manager software has been configured to report to the UNIX syslog or the Windows event log, an RSA Authentication Manager administrator can help detect and react to potential break-ins before they result in loss.

User Accountability

Damage may be done to valuable company information if a user's password is borrowed (without consent) or stolen. However, because logging on through the RSA Authentication Manager two-factor authentication process requires both the user's token code and personal PIN, it provides non-repudiation of his or her involvement in any unauthorized activities. The knowledge of this fact—and of the RSA Authentication Manager's comprehensive

reporting of all access to protected resources—helps users recognize their accountability for information security and behave accordingly. And while hackers often try to erase their footprints, the RSA Authentication Manager's access history logs can also be an important part of both investigating and building a legal case against a criminal.

Using Two-factor Authentication

Organizations can deploy RSA Authentication Manager software flexibly to protect corporate network resources in a number of ways. Protection can be comprehensive, authenticating all access to an enterprise network, or deployed strategically against specific sensitive resources. A single RSA Authentication Manager system can supply any or all of the following services:

- Authenticating remote user dial-in connections via a remote access server
- Authenticating VPN or firewall connections from the Internet to an internal network
- Authenticating all access to wireless LANs or wired corporate networks; can apply to all users, a particular workgroup or division, or only those of a certain access level
- Protecting sensitive data on intranets and extranets, by limiting access to web pages, URLs and directories
- Limiting access to mission-critical applications, sensitive files or other resources
- Preventing tampering with network administrative settings

Regardless of the scope of protection, the basic process of two-factor authentication is the same. When the user attempts to access the protected resource, the RSA Authentication Agent solution protecting that resource—the RAS server, wireless access device, web server, Windows environment or application—generates an authentication request. To gain access, the user must enter his or her user name, PIN and token code. The authentication request is encrypted and then forwarded to the RSA Authentication Manager.

Upon receiving the authentication request, the RSA Authentication Manager technology searches its user database and, when it locates the user name, compares the PIN and token code with its own records. If the combined PIN and token code are found to be valid, the user is granted access.

Which Authentication Solution?

	Category	The Solution: RSA Authentication Manager software with RSA SecurID Hardware Tokens
TCO	Acquisition	<ul style="list-style-type: none"> • Less expensive than smart cards or biometrics when you consider smart card + card reader + middleware, or biometric devices such as retinal scanners, fingerprint readers and associated software. • More expensive than passwords
	Deployment	<ul style="list-style-type: none"> • Deployment requires distribution of the hardware token only—there is no need to deploy software, drivers, readers or cables • Lower deployment costs than smart cards, biometrics or any other solution with client-side software that involves touching every end-user desktop • RSA Authentication Deployment Manager (bundled at no extra charge with a RSA Authentication Manager Enterprise Edition license) significantly lowers cost of deployment
	Management	<ul style="list-style-type: none"> • Significantly lower operational costs than passwords due to reduced help desk costs (See the white paper entitled “Authentication Scorecard: Passwords vs. RSA SecurID”) • Centralized administration eliminates need to manage multiple data stores
Fit (users)	Convenience / Ease of Use	<ul style="list-style-type: none"> • Eliminates need for user to remember multiple passwords • Easy to use—just type what you see • Similar in function to a banking ATM, the combination of a PIN and a device (the token) is easily accepted by users
	Portability	<ul style="list-style-type: none"> • Works anywhere—“zero footprint” solution
	Multi-purpose	<ul style="list-style-type: none"> • Single function—generates a new passcode every 60 seconds. However, a single hardware token can server as the means of access for multiple resources—the RSA SecurID Ready program provides out-of-the-box protection for over 295 applications from over 195 vendors, ranging from remote access to VPN to Wireless LAN to web-based resources.
Fit (corporate)	Relative Security	<ul style="list-style-type: none"> • Two-factor = very strong form of security • Passcodes cannot be guessed or predicted • Eliminates shoulder surfing and Trojan horse threats, as the token code changes every 60 seconds • Token codes cannot be easily detected as they traverse the network • Users are aware when a token is stolen or lost • Because passcodes are generated dynamically, they are not vulnerable to cracking tools • Improves security by eliminating the need to write down passwords • RSA Authentication Manager software provides logging and reporting functionality for greater end-user accountability • Centralized administration eliminates security holes as new devices, applications and communication methods are added and users are added, deleted, or change roles. • Provides “roles based” administrator access control
	Interoperability / Integration	<ul style="list-style-type: none"> • Interoperable with over 295 certified applications and products from over 195 Partners • Supports RSA SecurID authentication to Microsoft Windows online and offline • Unlike competitive partner programs, RSA SecurID Ready strategic partner products undergo extensive testing and documentation before being certified
	Robustness / Scale	<ul style="list-style-type: none"> • RSA Authentication Manager software scales to millions of users • Replication, fail-over capability and disaster recovery ensure high availability
	Future Flexibility	<ul style="list-style-type: none"> • Can be used to provide secure access to digital certificates • RSA SecurID has been adapted to dial-up, web, VPN and Wireless access methods and will continue to provide access control to new products through the SecurID Ready program.

V. FUNCTIONAL DETAIL

Architecture

RSA Authentication Manager software is used to establish a protective perimeter around selected network resources. The selection of which network assets are protected is up to the system administrator; the decision is made when the RSA Authentication Manager software is installed, but can be modified at any point. RSA Authentication Manager software does not have to be loaded on the network server; it can be installed on a wide range of Windows and UNIX server platforms. A single installation of the RSA Authentication Manager software can support more than one million users.

Each protected asset on the network is an agent and must run RSA Authentication Agent software. A single RSA Authentication Manager can host thousands of agents. RSA Authentication Agent technology is embedded in most networking equipment (routers, firewalls, VPNs, SSL-VPNs, Wireless Access Points, switches, etc.) and is also available for operating systems and web servers. Furthermore, the RSA Authentication Manager solution provides a multi-threaded agent API to facilitate custom built applications. Therefore, RSA Authentication Agent technology can be added or modified at any point, offering flexibility and scalability.

Whenever a network asset is accessed, the RSA Authentication Agent technology determines if the user login name is designated for RSA SecurID authentication and, if so, begins a two-factor authentication session. If the correct PIN and token code are provided, access is granted; otherwise the user is denied access.

System Components

The RSA Authentication Manager system consists of the following main components:

- A database of users, authenticators and RSA Authentication Agent software information, and a log database of user authentication attempts and administrator actions. The RSA Authentication Manager database is built on the Progress Software relational database, one of the world's leading OEM systems. The advantages of the Progress database are rapid access, allowing storage and authentication calls in the least possible time.
- The RSA Authentication Manager engine performs the user authentication based on the credentials supplied from an RSA Authentication Agent implementation. The

RSA Authentication Manager engine is the heart of the authentication process. Working in conjunction with the RSA Authentication Agent, the RSA Authentication Manager engine uses the database to verify the user and grant or deny access.

- An administration program, based on a graphical user interface, which allows the system administrator to manage the system—creating and changing settings, assigning authenticators and users and reporting. The RSA Authentication Manager administrative features and functions are detailed in the following section.
- Database replication and lock manager functionality for the prevention of replay attacks

The RSA Authentication Manager system includes many optional components including:

- An RSA Authentication Manager RADIUS server, which supports authentications using the RADIUS protocol and enables centralized administration of RADIUS users and profiles. The RADIUS server can run on the same machine as the RSA Authentication Manager or remotely.
- An RSA Authentication Manager TACACS+ server, which supports authentications using the TACACS+ protocol.
- A web-based help desk administration utility called Quick Admin

Database Replication and Load Balancing

One of the most compelling features of the RSA Authentication Manager solution is database replication. With database replication, security administrators are able to increase performance by configuring multiple Replica servers to simultaneously handle authentication requests.

RSA Authentication Agent software, using the version 5.x RSA Authentication Agent protocol provide automatic load balancing by detecting Replica server response times and routing authentication requests accordingly. Customers can also define their own load balancing sequence by defining a pick list in the Server configuration file. RADIUS users can do the same using RADIUS hunt groups.

With an RSA Authentication Manager Base license, customers can deploy a set of one Primary server to handle administration and authentication and one Replica server to also handle authentications. With an RSA Authentication Manager Advanced license, customers can deploy up to 6 sets (realms) each with a Primary and up to 10 Replica servers. This architecture not only guarantees availability, but also allows customers to plan efficient, economic global network topologies. Further features and benefits of an RSA Advanced license are discussed below.

Pre-5.x RSA Authentication Agent software can be configured to point to two Replica servers.

Each Replica server contains a complete copy of the user database. If the Primary server should fail, a Replica server can be easily promoted to be a new Primary server quickly restoring administration and full replication.

Lock Manager

To detect and prevent replay attacks, RSA Authentication Manager technology includes a lock manager process that runs on each server. When a user logs into a Replica server, the lock manager on that server immediately sends a lock request to every other server in the realm, thereby blocking the user's token and token code from reuse.

System Communications

For reliable communication between the Primary and Replica servers, the RSA Authentication Manager software uses TCP. The data stream is encrypted and the encryption key changes every ten minutes.

Communication between the RSA Authentication Manager software and RSA Authentication Agent software uses a combination of UDP and Unicast, for maximum speed. Data packets are encrypted, each with a different key, to protect against eavesdropping and masquerading.

Encryption

Each RSA Authentication Agent implementation in the system has a unique key, or "node secret." A node secret is a string of pseudo-random data known only to the client and server. The node secret is used to encode and decode communications. The RSA Authentication Manager software creates the node secret for each RSA Authentication Agent implementation. After the RSA Authentication Agent implementation obtains the user's PIN and token code, this information is encrypted using the node secret and other information unique to the authentication and sent to the RSA Authentication Manager software.

Time Synchronization to UCT

Universal Coordinated Time (UCT) is used to synchronize all RSA Security products. Each RSA SecurID token is set to UCT (identical with Greenwich Mean Time) before it is shipped to a customer; during installation, the RSA Authentication Manager system clock is likewise set to UCT. In essence, all RSA Security products the world over are set to the exact same clock, eliminating the need to deal with differences between time zones or daylight savings adjustments.

Valid Token Time Window and Clock Drift Adjustment

To account for slight discrepancies in time settings and clock drift when using hardware based tokens, the RSA Authentication Manager software is designed to authenticate based on a three minute time window: the current time on its UCT clock, as well as the minute before and the minute after. If the user name and PIN are accurate, but the token code provided does not match the current minute, the RSA Authentication Manager software automatically checks to see if it matches the correct code for the previous or subsequent minute. This procedure accommodates the situation where the clock in the authenticator has drifted slightly out of phase with the clock in the RSA Authentication Manager system. If a match is found with the prior or following token code, the user is authenticated and a note is made in the user's database record to adjust future logins to reflect the time drift. Attempts to re-use recently used token codes are detected and logged. Attempting to use a very old token code is prevented because the Server only allows a few token codes to be valid for any single authentication.

Provided a user logs on regularly, the RSA Authentication Manager software will keep the token's time adjusted so that the token code always falls within the three minute window. However, if a user does not log on for an extended period (typically for many months), the token time could drift outside the three-minute window, generating a token code not recognized as valid. In this case, the RSA Authentication Manager software checks the token codes for the 20 minutes ahead of and behind the current minute. If the token code is found to match one of these codes, the RSA Authentication Manager software requests a second token code from the user, to verify possession of the token; if this second token code shares the same clock drift, the token is assumed to be valid. The user is authenticated and the RSA Authentication Manager software notes that particular authenticator's clock discrepancy in its user record for future logins.

If, however, the supplied PIN does not match, or an erroneous token code is entered that cannot be explained by clock drift, the RSA Authentication Manager technology requests a second attempt from the user. Administrators can set the number of retry authentication attempts to allow before locking out the user and creating an alert log entry.

While the RSA Authentication Manager software follows the same process for authenticating all RSA SecurID token codes, the clock drift allowances for the RSA SecurID token are slightly greater, allowing for more drift in the clocks that reside in personal computers and PDAs.

Support for Mobile Users

If during authentication, the RSA Authentication Manager software does not recognize the supplied login, it can be configured to automatically query other RSA Authentication Manager realms protecting an enterprise network or specific e-business applications. Each realm consists of an RSA Authentication Manager Primary and one or multiple Replica servers which all share the same user and log database. This database is replicated among servers in a realm.

If a user is native to one realm but attempts to access a resource, which is protected by an RSA Authentication Agent, which passes authentication requests to a different RSA Authentication Manager realm, a cross-realm enterprise authentication operation takes place transparently to the user. If this user is identified by one of the network's other RSA Authentication Manager realms as a valid Remote User, the authentication request will be forwarded to that RSA Authentication Manager realm for validation.

Once authentication is successful, the local RSA Authentication Manager realm caches the user's home realm information locally, in order to expedite future logins. This avoids the need to create duplicate user records in each RSA Authentication Manager realm on the enterprise network, preventing a situation where the user leaves the company but a phantom user record still exists in a different Primary RSA Authentication Manager realm.

Support for multiple realms and establishing cross-realm relationships requires an RSA Authentication Manager Advanced license. For more detail on RSA Authentication Manager Advanced, see the discussion below.

Managed Authentication Services

Many organizations are interested in adding two-factor user authentication to their networks, but simply do not have the infrastructure or resources to deploy and maintain it. As an alternative, many leading Service Providers now offer RSA SecurID authentication as a part of their remote access, VPN, firewall or managed security services. Depending on the degree of control the customer seeks, the RSA Authentication Manager technology can either be located at the Service Provider network, or can be hosted and managed by the Service Provider at the customer premise. Some Service Providers additionally offer an RSA SecurID Software Token as a built-in component of the dialer of a VPN client on the user desktop.

When a company uses an RSA Authentication Manager hosted at a Service Provider network, the server authenticates remote access users before creating a secure tunnel with the corporate network.

Interoperability

Through the RSA SecurID Ready program, the RSA Authentication Manager solution is instantly compatible with the industry's leading security and networking products. Over 270 products from 185 RSA SecurID Ready strategic partner are interoperable with RSA Authentication Manager. For a complete list of RSA SecurID Ready strategic partner, refer to www.rsasecurity.com/partners/secured/securidpartners.html.

One of the benefits of this advanced interoperability strategy is that companies can leverage the infrastructure already in place, safeguarding existing investments.

Investment Protection

Should you want to add even stronger authentication to your network (such as using RSA SecurID to protect PKI credentials), you can simply build on your RSA SecurID solution already in place. RSA Authentication Manager works seamlessly with the RSA Keon PKI solution. For example, an RSA SecurID token can be required to protect access to a certificate on a desktop or in a virtual credential store such as that provided by RSA Keon Web Passport or RSA SecurID can be used to unlock a smart-card credential.

VI. RSA AUTHENTICATION MANAGER ADMINISTRATION

RSA Authentication Manager software includes a number of features to enhance both operational and security administration functions.

Security Administration

Comprehensive administrative features are accessible via a graphical user interface that is intuitive and easy-to-use, minimizing training requirements. Administrators can choose any Windows desktop console.

Alternatively, a web-based utility called Quick Admin allows the security administrator to modify the user and token information without installing an admin client on every desktop. Targeted at first tier help desks, Quick Admin provides an intuitive web-based interface for the most common user and token management tasks (such as PIN resets, deactivating lost tokens and assigning new tokens).

RSA Authentication Manager technology supports the use of an LDAP directory as the centralized, authoritative source of user information. User and group information can be centrally managed in an LDAP directory and imported into the RSA Authentication Manager database automatically through a schedulable synchronization job, while authenticator information is securely stored and managed only through the RSA Authentication Manager software.

Users may be assigned into groups for applying security policies, thereby easing the administrator's role. For example, login for any user or group can be restricted by the time of day or day of the week as well as to specific agents. With a simple exercise, the administrator is able to restrict access by a distinct group of users or targeted individuals from a central point.

Administrative authority can be delegated through the creation of administrative roles throughout the organization. Using this feature, assignment of new tokens can be handled locally, while access policies are managed centrally. Realms can also be administered from either a central or remote location.

As an option, RADIUS profiles and passwords can be managed centrally through RSA Authentication Manager, providing a single point of authentication and administration.

Token Assignment and Replacement

With the RSA Authentication Manager software, token management is a centralized and efficient process. A point-and-click interface for setting up users and groups, assigning and deleting authenticators and defining access parameters greatly simplifies the administration of

authenticators. Expiring tokens can be replaced in batch, automating a repetitive and often time consuming task.

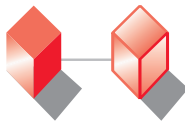
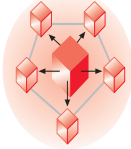
New users can be added to a database at any time and the RSA Authentication Manager software automatically prevents duplication of user IDs.

These features, combined with a comprehensive lifetime warranty on tokens, significantly eases the task and lowers the overall cost of managing and maintaining the system.

Automated, Browser-based Credential Deployment

A web-based workflow system, RSA Authentication Deployment Manager software helps reduce administrative costs by offering end users a self-service platform to request, activate and initiate deployment of RSA SecurID credentials. The system automates the entire credential deployment process—including populating the RSA Authentication Manager database with user data, token assignment and activation and facilitation of the fulfillment of RSA SecurID token requests. Manual assignment of a user to a token is no longer required. Any token can be sent to any user as the RSA Authentication Deployment Manager software programmatically handles the process of binding a user to his token. The only administrative involvement is the credential approval and actual distribution of the credential to the end user. Flexible and scalable, RSA Authentication Deployment Manager solution is ideal for both enterprise and e-business related deployments, making issuing credentials faster, more efficient and easier than ever.

RSA Authentication Deployment Manager software is included with an RSA Authentication Manager Enterprise Edition license and available at additional cost with an RSA Authentication Manager Base license.

<p>RSA Authentication Manager License Types</p>	 <p>Base</p>	 <p>Enterprise Edition</p>
<p>Number of authenticating servers</p>	<p>1 primary, 1 replica</p>	<p>1 primary, up to 10 replicas in each realm</p>
<p>Number of realms (group of primary & replica servers)</p>	<p>1 realm</p>	<p>Up to 6 realms</p>
<p>Support for high availability systems*</p>	<p>No</p>	<p>Yes</p>
<p>RSA Authentication Deployment Manager</p>	<p>Extra cost</p>	<p>Included</p>

Logging and Reporting

RSA Authentication Manager software also supports notification based on events. Select messages from the RSA Authentication Manager audit log can be forwarded to the UNIX syslog or Windows event log, calling attention to the most important events from the system's extensive log data.

With RSA Authentication Manager software, an audit trail of each login attempt and operation performed is automatically generated. Audit trails extend to the user, which helps prevent losses from insider abuse or employee laxness regarding security policies. The automated log maintenance feature lets administrators create settings for archiving log files. This "set and forget" feature ensures that usage logs are safely preserved without intervention.

RSA Authentication Manager software allows administrators to easily tailor reports according to their own security requirements. Reports can be designed to view an activity, exception or incident, as well as usage summaries.

Other Features

RSA Authentication Manager software provides many other features to enhance its overall functionality including an online documentation and help facility and an administrative toolkit that allows administrators to interface with administrative functions.

VII. RSA AUTHENTICATION MANAGER ENTERPRISE EDITION LICENSE

An RSA Authentication Manager Enterprise Edition license can bring significant benefit to an enterprise by enabling risk reduction, cost savings and compliance with policy.

Differences in the RSA Authentication Manager licenses

The ability to support up to 11 authenticating servers, gives RSA Authentication Manager Enterprise Edition license customers the benefit of reduced risk of authentication downtime. Network failure, server failure and single point of failure during maintenance can all be addressed through multiple redundant authenticating servers.

Multiple realms allow RSA Authentication Manager Enterprise Edition license customers to configure up to six installations of RSA Authentication Manager software (1 Primary and up to 10 Replica servers in each) each with distinct replicated user and log databases. Cross-realm relationships can be established which allow an RSA Authentication Manager realm which does not recognize the supplied login to automatically query other RSA Authentication Manager realms for validation.

Multiple realms and multiple Replica servers enable an RSA Authentication Manager Enterprise Edition license to provide customers with the flexibility to efficiently and securely deploy RSA SecurID technology into their global network. Customers can place Replica servers near users in different regions thereby reducing transcontinental network charges and traffic and increasing performance. Customers also may separate US, European and Asian employees into two locally administered realms while maintaining worldwide access for roaming employees.

The flexibility enabled by an Enterprise Edition license of RSA Authentication Manager software helps enterprises to comply with administration and security policy. Companies of any size may have distributed administration requirements (i.e. they have separate business units or subsidiaries) that necessitate the placement of groups of users in separate databases (i.e., realms). Some governmental regulations require customer or employee data to be stored on databases in countries with adequate privacy protection legislation.

An RSA Authentication Manager Enterprise Edition license allows a company to design their RSA Authentication Manager deployment and network configuration to scale as more users and projects make use of RSA SecurID authentication. As users and projects are added, load balancing among additional authenticating servers results in sustained high performance and a continued positive end user experience.

RSA Authentication Deployment Manager (included with an Enterprise Edition license and described above) software enables a self-service token provisioning model that reaches any user, anywhere.

To ensure maximum uptime and reduce the risk of downtime, RSA Authentication Manager Enterprise Edition software is certified to run on Veritas Cluster Server high availability platform on Solaris. By running the Primary RSA Authentication Manager on a high availability system, administrators can be confident that their RSA Authentication Manager Primary solution will always be available for administration and database reconciliation.

VIII. CONCLUSION

RSA Authentication Manager software is a key component of the RSA SecurID two-factor authentication solution. Using RSA SecurID technology, companies can prove the identity of your employees, strategic partners and customers as they do business together. Greater confidence in user identity enables companies to make more valuable applications and data available remotely and online increasing revenues and decreasing costs while mitigating risk and ensuring compliance with governmental, industry, or enterprise regulations.

Limiting access to authorized users is an important element in protecting enterprise information, systems and resources. Losses resulting from security breaches are among the most expensive and disruptive of information crimes. Consequently, it is critical that companies invest in a high performance authentication solution that scales to protect mission critical applications across the enterprise. The RSA SecurID two-factor authentication solution, including RSA Authentication Manager software, offers a high performance means for preventing these losses. The solution is extremely scalable and flexible and can be deployed in multiple ways: protecting specific assets, protecting files and applications, or protecting all access to enterprise networks.

The RSA Authentication Manager software is broadly supported by connectivity equipment and software vendors, making it the most interoperable of any authentication solution on the market. Not only does it protect existing infrastructure investments but also it provides the flexibility companies need for the future.

IX. ABOUT RSA SECURITY

Mission

As mentioned previously, effective security solutions must not only focus on “keeping the ‘bad’ guys out,” but also on enabling business processes and providing competitive advantage. In fact, security needs to enable business processes and begin to provide competitive advantage. Specifically, Identity and Access Management solutions, such as RSA Authentication Manager software, can make organizations easier to do business with, by creating cross-selling opportunities online and enabling new methods of conducting business. RSA Security’s mission is to work with our customers to transform identity and access management solutions into a catalyst for competitive advantage.

Singular Focus: Identity and Access Management

RSA Security is uniquely positioned to address any organization’s identity and access management needs—today and in the future. RSA Security’s heritage is in authentication, authorization and administration—the foundation of evolving identity and access management technology. In fact, the Company already offers a comprehensive family of solutions to address today’s identity and access management challenges. More importantly, RSA Security offers a vision and migration path toward an identity and access management platform that will effectively address future requirements on a single platform that integrates transparently across heterogeneous e-business infrastructures.

With thousands of customers, spanning nearly two decades, RSA Security understands the needs of the security market. The Company studies and internalizes its customers’ current and emerging needs to ensure the development of effective identity and access management solutions. As customers’ e-business initiatives evolve over time, RSA Security will be their strategic security partner, helping to transform identity and access management technology into a catalyst for competitive advantage.

Industry Leader

With a solid customer base and over one billion RSA-enabled software units shipped, RSA Security is a trusted, experienced partner that will continue to innovate and educate in order to best meet its customers evolving e-business challenges. RSA Security has focused solely on e-security—specifically, identity & access management—for nearly two decades. The Company is a pioneer in strong authentication, encryption and digital certificate management solutions and has emerged as an innovator in access management. Over this time, RSA Security’s

ingenuity has led to a 70% market share in strong two-factor authentication and a population of users under the protection of RSA cryptography that spans virtually the entire Internet. RSA Security also leads the development of industry standards, such as the Liberty Alliance Project, SAML and PKCS. The Company's efforts ensure that customers working with RSA Security truly get the right solution for their heterogeneous environment and growing business. In addition, RSA Security's unrivaled leadership role is evidenced by the widespread popularity of our informational platforms: including RSA Conference (the largest security event in the world), RSA Laboratories (the research center of the company) and RSA Press (a publishing initiative focusing on information security books).

Advocate of e-Business

RSA Security continues to work with its customers to deliver business value, transforming identity and access management solutions into opportunities for competitive advantage. The Company's portfolio of e-security solutions are designed to help organizations fully realize the revenue opportunities, operational improvements and customer service benefits of e-business—while protecting critical resources and applications from unauthorized access and other forms of electronic malice. In fact, RSA Security boasts thousands of customers around the world who already use our identity and access management solutions to contribute significantly to their bottom line by improving their business processes with increased revenue, enhanced customer satisfaction and lower costs. As identity and access management increasingly becomes a strategic imperative for many organizations, RSA Security will strive to offer its customers competitive advantage through enhanced security.

Seamless and Transparent Solutions

RSA Security continues to provide solutions that fit seamlessly into customers' heterogeneous e-business infrastructures. RSA Security boasts the strength of more than 1,000 technology partnerships with industry powerhouses that allow the Company to integrate its solutions into virtually any environment. The RSA Secured® technology partner program, a key part of this initiative, focuses on product integration and certification activities as well as joint support strategies for our mutual customers. Our RSA BSAFE developer solutions enable developers to quickly and effectively integrate key security standards for encryption, application integration and electronic signatures into their applications. Most importantly, RSA Security not only leads industry standards development activity, but is also committed to implementing these standards into its products to achieve optimal integration for its customers. The Company's current products support a multitude of standards, including PKCS, RADIUS and the OASIS SAML (Security Assertion Markup Language) 1.0 specification. Through its technology partnerships and standards initiatives, RSA Security is in a unique position to represent its customers and their preferences in the creation of technology solutions that best fit their needs.

Superior Service

With sales and support offices in all the major international regions, RSA Security is able to fully understand the unique requirements of each local geography and funnel that information directly to our product development teams. RSA Security provides expert advice and quick answers to keep customers up and running—every minute of every hour of every day—with 24x7 support from offices located around the world. Additionally, RSA SecurCare® On-line is a web-based support offering that facilitates anytime, anywhere access to critical support information including software updates, bug fixes, service alerts and documentation.



RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

RSA, RSA Security, the RSA logo, RSA Secured, SecurID and the RSA Secured logo are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.
 ©2004 RSA Security Inc. All rights reserved.

AS51 TB 0904