



The Security Division of EMC

White paper

The Authentication Scorecard



"Which authentication technology should I use?"

RSA addresses this recurring question by providing a consistent, structured framework and a corresponding tool – the Authentication Scorecard – that helps organizations to understand, evaluate and select the most appropriate authentication technology – or technologies – from among a wide selection of alternatives.

RSA leverages the Authentication Scorecard to help customers and prospects make sense of the many available options in a consistent, structured, apples-to-apples framework, and ultimately to narrow the selection of authentication solutions to those that strike the ideal balance among multiple objectives based on your priorities. This white paper provides an overview of the Authentication Scorecard and a framework for objectively analyzing authentication options.

Contents

I.	The Need for Authentication	page 1
II.	Understanding the Authentication Options	page 2
III.	Using the Authentication Scorecard	page 2
IV.	Analyzing the Authentication Attributes	page 4
	Total Cost of Ownership	page 4
	Strategic Fit – User Requirements	page 4
	Strategic Fit – Corporate Considerations	page 5
V.	Weighing Attributes Based on Priorities	page 5
VI.	Quantifying Alternative Solutions	page 6
VII.	Summary	page 7
	Appendices	page 7
	Appendix A – Passwords	page 8
	Appendix B – RSA SecurID Hardware Tokens	page 9
	Appendix C – RSA SecurID Software Tokens	page 10
	Appendix D – RSA Digital Certificates	page 11
	Appendix E – Hybrid One-time Password USB Tokens	page 12

I. The Need for Authentication

Protecting access to information is essential to securing enterprise information assets, and authentication – proof of identity – is a necessary element of all enterprise security initiatives. Selecting the optimum authentication solution – or solutions – can become an increasingly complex decision because of the range of alternatives available.

Remote access to enterprise information has been a primary driver for authentication, but organizations today face other drivers, including compliance requirements, the need to secure Web-based applications, the demands of protecting Wireless LANs (WLANs) and the productivity advantages of enabling single sign-on to multiple applications.

For some applications and for some user groups, the use of passwords can be sufficient. For example, administrative employees with limited access to mission-critical applications can often have their identities secured with password-only authentication. But other user groups such as the following require stronger authentication:

- Executives with access to critical applications
- Sales/support reps who have access to customer information
- Financial, human resources or IT professionals who have access to sensitive personal information
- Business partners with access to sales, competitive, pricing and customer data

Authentication is no longer essential just for remote access, but it is also needed to ensure that users within the enterprise are indeed who they claim to be. Organizations need to protect the identities of desktop users as well as remote workers, which is becoming an even greater challenge as companies extend the network to business partners, suppliers and customers.

Whether a user accesses the network from the desktop or from a PDA or remote access connection, the organization needs to make trade-offs to select the method of authentication that provides the ideal mix of ease-of-use and security. Decisions on authentication technology become increasingly complex because of the wide range of options available, and objective measures are needed to evaluate authentication options. The access characteristics of user segments need to be carefully evaluated, and organizations must also assess the value of the data that various user communities will access.

For many companies, multiple authentication options can be selected based on such metrics as the need for portability and the importance of the information a given user group can access. Cost is certainly a consideration, and organizations should evaluate acquisition costs, deployment and help desks costs. For example, passwords are the least expensive to acquire and deploy but result in high ongoing operational and help desk costs.

Evaluating the Alternatives

If you are interested in using the Authentication Scorecard, contact your RSA sales representative or an authorized RSA Channel Partner, or visit www.rsa.com, click on "Contact" then click on "Sales Contact Request". When you fill out the request form, please indicate in the comments section that you are interested in the Authentication Scorecard. You will be contacted shortly after submitting your request.

The RSA representative will ask you to weigh the relative importance of ten attributes, and then send you a chart that graphically compares the relative weight of each attribute and displays the results in a form that you can use to evaluate multiple alternatives based on multiple criteria. The chart is used to analyze the relative strength and weaknesses of alternative strategies, allowing organizations to make logical comparisons between alternative solutions.

Passwords have always been recognized as providing relatively weak security, but the proliferation of passwords has become unmanageable for end users and administrators alike, and the authentication method once naively viewed as "free" is actually surprisingly expensive in terms of ongoing management and support costs.

Conversely, organizations can authenticate users based on something they know – a personal identification number (PIN) – and something they have – the constantly changing code on a hardware or software token that is synchronized with a centralized authentication manager. Two-factor authentication provides much better security than passwords and is less expensive to operate, but two-factor authentication solutions are more expensive to deploy and require organizations to evaluate and select from diverse token options.

Weak, password-based authentication contrasts sharply with stronger authentication methods, and organizations opting for an alternative need to carefully evaluate the advantages and disadvantages of each option to select the right solutions.

II. Understanding the Authentication Options

RSA developed the Authentication Scorecard so organizations could weigh authentication options. This spreadsheet-based tool allows companies to compare and contrast authentication options. The Authentication Scorecard allows you to evaluate the relative strength and weakness of the following authentication options:

- **Passwords**, which are inexpensive to deploy but expensive to manage and support. They offer the weakest security because they can be easily hacked, guessed or stolen.
- **Hardware Tokens**, which are small enough to attach to a key chain and generate a constantly changing one-time password to enable two-factor authentication.
- **Software Tokens on PCs**, which enable two-factor authentication but are less portable.
- **Software Tokens on Mobile Devices**, which allow authorized users to gain two-factor authentication from smart phones and PDAs for mobile access to enterprise information.
- **Digital Certificates**, which contain user identities and enable the centralized management of cryptographic keys.
- **Smart Cards with Digital Certificates**, which enable the integration of physical access and logical access via card-based authenticators that contain digital credentials.
- **USB Tokens with Digital Certificates** that can be plugged into a standard USB port to enable cryptographic authentication.
- **Hybrid One-Time Password USB Tokens** that can be plugged into a standard USB port to enable two-factor authentication without the need to key in a token code. They can also contain digital certificates.
- **Biometric Devices**, which enable authentication according to the physical characteristics of a user. Examples include fingerprint identification and retina scans.

The Appendices to this document contain authentication snapshots for many of these options, and to evaluate all of these options contact your RSA representative.

III. Using the Authentication Scorecard

The Authentication Scorecard helps organizations select the authentication solution (or solutions) best for their own unique needs. It helps organizations understand, evaluate and select the most appropriate authentication technology from among this wide selection of available alternatives.

Why an Authentication Scorecard? In light of expanding methods and technologies for gaining access to enterprise applications, the increasing value of information and the operational and the security limitations of passwords, companies are frequently re-evaluating their authentication strategies. But with so many authentication alternatives available, how can they objectively be evaluated? Vendors who sell a single authentication technology may not be the most objective source of information – for as the saying goes, "when all you have is a hammer, everything looks like a nail".

Of particular challenge is the fact that the market buzz about certain authentication technologies does not always equate to the market realities about how widely those technologies are actually deployed. Biometric solutions, for example, enjoy a disproportionate share of media coverage relative to their actual deployment. They require expensive and often cumbersome readers that are largely impractical for mobile or remote access, so they are used by only a small subset of the market.

Vendors that quite naturally emphasize only the strongest aspects of their particular solutions tend to exacerbate the problem by creating – either directly or indirectly – apples-and-oranges comparisons between various authentication technologies. For example, how can one objectively compare the multi-purpose value proposition of a "smart badging" solution (i.e., combining photo ID, building access, network/application access and stored values on a single physical device) with the low-cost, zero-footprint, zero-deployment value proposition of a one-time passcode.

At RSA, our belief is that there will be no one silver bullet for all authentication problems, no single technology or approach that will optimally address all scenarios, no universal solution that will meet all requirements. On the contrary, there will continue to be a rich diversity of authentication technologies used based on company priorities, budgets and security demands.

RSA develops, sells and supports solutions designed to work with a range of authentication technologies, from traditional time-synchronous tokens, to digital certificates, to smart cards and USB tokens, to virtual credentials and

Categories	Attributes	Questions to Ask
Total Cost of Ownership	Acquisition Cost	<ul style="list-style-type: none"> – What are the initial acquisition costs? – Include all additional hardware, software, servers, readers, services, etc. associated with acquiring the authentication solution.
	Deployment Cost	<ul style="list-style-type: none"> – What are the costs to deploy the authentication solution? – This includes the distribution of any necessary hardware or software; ease of installation; ease of setup and configuration; training of end users; etc.
	On-going Management Cost	<ul style="list-style-type: none"> – What are the ongoing operating costs? – This may include costs for replacement (e.g., expired / lost / stolen / broken) authentication devices; ongoing management; upgrades; vendor support; help desk support; etc.
Strategic Fit (users)	Convenience/Ease of Use	<ul style="list-style-type: none"> – What kinds of end user population(s) will be supported? – How easy is it for end users to learn how to use the authentication method? – How convenient is it for end users to use the authentication method, day in and day out?
	Portability	<ul style="list-style-type: none"> – How portable is the authentication method? – Can it reliably be used to gain access from multiple locations (office, home, airport, hotel, etc.)?
	Multi-Purpose	<ul style="list-style-type: none"> – Can the authentication method be used for more than one purpose? e.g., network access, physical access, application access, photo ID badge, electronic signature, stored value, etc.? – Does the authentication method leverage a device that is itself used for multiple purposes, e.g., PC, PDA, phone, etc.?
Strategic Fit (corporate/system)	Relative Strength	<ul style="list-style-type: none"> – How strong is the authentication? – How secure is the implementation? – Is it adequate for the information being protected? – Does it meet regulatory requirements (if any) for the protection of information?
	Interoperability/Back-end Integration	<ul style="list-style-type: none"> – Does the authentication solution work natively with multiple products? – Does it work only with the installation of additional software? – How easy is it to integrate with back-end resources or applications? What resources and applications need to be supported?
	Robustness/Scale	<ul style="list-style-type: none"> – Does the authentication solution scale to the degree required now? – Three years from now?
	Future Flexibility	<ul style="list-style-type: none"> – What future options may be available from the selection of this authentication solution (whether you currently intend to use them or not)? – What future options might be of interest?

The Authentication Scorecard identifies three high-level categories that can be broken down into the 10 key attributes to measure.

virtual containers and even passwords. The Authentication Scorecard was developed to provide the industry with a consistent, structured framework that helps organizations to understand, evaluate and select the most appropriate authentication technology from a broad cross-section of alternatives.

IV. Analyzing the Authentication Attributes

Ultimately, selecting the appropriate authentication solution is a trade-off among three variables:

- Security
- Cost
- Convenience

The Authentication Scorecard is an updated and expanded framework that reflects not only RSA's years of experience and market leadership in strong authentication technology, but also the additional structure and detail required to make an apples-to-apples-rather than apples-to-oranges-comparison of various authentication technologies.

In the Authentication Scorecard framework, there are three high-level categories, each of which can be broken down further for a total of ten basic attributes. Any authentication technology can be compared – in a consistent manner – using this simple framework.

The following table outlines the Authentication Scorecard framework, including a series of basic questions that can be used to compare and contrast various authentication alternatives. The Appendices later in this document then use this framework to give an objective assessment of the leading authentication solutions.

Total Cost of Ownership

	Products/Technologies	People	Process	Plant/Facilities
Acquisition Cost				
Deployment Cost				
On-going Management Cost				

Acquisition, deployment and maintenance costs can be carefully evaluated to determine the total cost of ownership of alternative authentication technologies.

Cost is a critical consideration, but the enterprise needs to consider all the elements of cost – too often, the focus is on acquisition cost alone. For example, passwords are "free" in terms of acquisition cost, but they are surprisingly expensive in terms of ongoing management and support costs. Fortunately, the total cost of ownership can be reasonably well quantified. Using the questions in Table 1 as a starting point, one could readily estimate costs based on the simple 3x4 matrix in Table 2.

Strategic Fit – User Requirements

Depending on the specific user populations under consideration (employees, business partners, customers and various sub-segments of each), the requirements for convenience and ease of use may vary. Some user populations will expect simple passwords for access, but many organizations will want stronger authentication for employees that access mission-critical applications.

Portability will also vary by user population and is often tightly linked to cost. For example, solutions that require the installation and support of client-side software are generally more costly and may also limit portability. The enterprise has to ask questions such as:

- Are all the required readers, software, drivers, cables, etc. available at work?
- At home?
- At airports?
- In hotels?
- In kiosks?

Portability can be a factor in other ways as well – for example, solutions that send one-time passcodes to a mobile device such as a smart phone or PDA are extremely portable, provided that the end user is in a coverage area for the text-delivery service.

Some authentication solutions are based on single-purpose devices; authentication is all that they do. Other solutions feature a multi-purpose value proposition in one of two ways because it might:

- Combine multiple functions in a single device (e.g., photo ID, building access, network credentials and stored values).
- Be based on a device that the end user already relies on for other purposes (e.g., a phone or PDA).

Strategic Fit – Corporate Considerations

The matters of relative security, interoperability/back-end integration, robustness and scale are relatively straightforward based on the questions in Table 1 and the solution-specific examples provided in the Appendices, but the future value of an authentication solution must also be considered.

One example of future flexibility can be found when considering digital certificates, a solution which might be used today for user authentication – and which has the potential to be leveraged in the future for encryption and for digital signing. The ability to federate identities using common credentials is another potential future value of an authentication solution.

For example, employees might use their credentials today to access enterprise resources, but in the near future you may also want employees to have the flexibility to use that same credential to access the applications of a partner or customer. Organizations should evaluate immediate authentication requirements as well as future potential authentication requirements to select the solutions that meet both the immediate and long-term security requirements of the enterprise.

V. Weighing Attributes Based on Priorities

A consistent, structured framework is needed that will help organizations understand, evaluate and compare a wide range of alternative authentication technologies. This is necessary, but not sufficient. Management needs to select the most appropriate authentication technology for users, applications, company requirements, industry best practices and regulatory requirements.

Context is crucial, and different organizations will weigh these categories and attributes based on their own business priorities. For example, "Company A" may value portability, high security and integration above all other requirements, while "Company B" may most highly value multi-purpose solutions, good security and future flexibility.

Both of these organizations can leverage the same Authentication Scorecard to understand, evaluate and compare various authentication alternatives, but they would naturally apply different weights to the ten basic attributes. They are likely to select different authentication solutions, and the Authentication Scorecard provides a framework for objectively analyzing attributes and selecting the ideal authentication solutions for business requirements and priorities.

Solution Attributes	Customer-specific Weights	Solution-specific Values
Acquisition Cost	%	1 – 10
Deployment Cost	%	1 – 10
On-going Management Cost	%	1 – 10
<hr/>		
Convenience / Ease of Use	%	1 – 10
Portability	%	1 – 10
Multi-purpose	%	1 – 10
<hr/>		
Relative Security	%	1 – 10
Interoperability / Integration	%	1 – 10
Robustness / Scale	%	1 – 10
Future Flexibility	%	1 – 10
	<hr/>	<hr/>
	100 %	X
		←= 100 % = SCORE

The Authentication Scorecard offers a quantitative selection approach that allows organizations to analytically measure the value of authentication alternatives to their business.

VI. Quantifying Alternative Solutions

The qualitative approach to the Authentication Scorecard previously outlined is useful and illustrative, but many customers ask if there is a more quantitative approach. The answer is yes – RSA has developed a more quantitative model based on the general approach outlined in Table 3.

Each authentication solution under consideration is given a numerical score between 1 and 10 for each of the ten basic attributes of the Authentication Scorecard. Higher scores are better, so a score of 8 is better security than a score of 3, and a score of 8 is lower than a score of 6. If a particular solution got numerical scores of 10 for all 10 categories, the maximum sum of all scores would be 100. However, this is not a likely scenario because of the trade-offs involved in assigning scores to each category. Scores are admittedly somewhat subjective, and one could easily debate whether a particular solution should have received a "6" or a "7" in a given category. The predetermined scores represent the best judgment of the product management team at RSA.

Next, based on a discussion with the RSA representative and information about your user population(s), application(s) and company as well as industry-specific considerations, a percentage weight must be assigned to each of the ten basic attributes of the Authentication Scorecard.

Higher percentage values indicate higher weights, and all weights must add up to exactly 100%. This last part is critical; it forces the relative ranking of the ten basic attributes against one another, which is required for the quantitative approach.

For example, if you cared about relative security above all else, you would assign 100 percent to that attribute and therefore assign 0 percent to everything else. However, most companies have a balance among several attributes, and therefore need to distribute the weighting among the various elements, giving more weight or less weight to individual elements to reflect their user-specific, application-specific, company-specific and industry-specific preferences and priorities. In our experience, this part of the exercise has proven to evoke some of the most interesting and ultimately highly useful internal discussions as organizations articulate, define and prioritize their authentication priorities.

After you assign values to attributes that total 100 percent, the RSA representative can provide you a visual chart for each alternative and a comparison matrix that visibly demonstrate the weighting of each attribute. You can then more carefully analyze authentication options and select the right authentication solution – or solutions – for your organization.

VII. Summary

Based on our experience in using this tool, we have found that it is most effective when someone who is familiar with it guides its initial use – after which it makes an excellent tool for ongoing evaluation, discussion and narrowing down of specific authentication solutions.

By investing just a few minutes in our established Authentication Scorecard, you can gain sharper insights into the trade-offs involved in selecting the optimum authentication solution(s) for your organization and receive visual charts that graphically display the value of each option analyzed based on your input and the insights of authentication experts. You will also receive an easy-to-use matrix that graphically displays the weight you assigned to each of the criteria. This matrix can help you make the right security decisions for your organization based on your business priorities and security requirements.

The Authentication Scorecard helps organizations to understand, evaluate and select the most appropriate authentication technology or technologies from the range of available options. We have been using it successfully to help our customers and prospects make sense of the many available options in a consistent, structured, apples-to-apples framework, and ultimately to narrow the selection of authentication solutions to those that strike the ideal balance for their multiple objectives. Additional information and quantitative tools on this important topic are readily available from RSA representatives.

Read the attached appendices for summary results of the most popular authentication options that highlight key points in each of the three categories for each of the ten attributes. For additional information about using our interactive Authentication Scorecard spreadsheet to evaluate your authentication options, contact your RSA sales representative or channel partner or visit www.rsa.com and click on "contact".

Appendices

- Appendix A: Passwords
- Appendix B: RSA SecurID® Hardware Tokens
- Appendix C: RSA SecurID Software Tokens
- Appendix D: RSA Digital Certificates
- Appendix E: Hybrid One-Time Password USB Tokens

Additional Information

For additional information about using our interactive Authentication Scorecard spreadsheet to evaluate your authentication options, contact your RSA sales representative or channel partner or visit www.rsa.com and click on "contact".

Appendix A – Passwords

Total Cost of Ownership Considerations

Acquisition Cost

- Passwords are “free” in that there are no acquisition costs – but they are expensive when considering deployment and management costs.

Deployment Cost

- No hardware or software to deploy.
- Often times companies opt to purchase password synchronization or single sign-on products in an attempt to ease the end user burden of multiple passwords.

Management Cost

- The average user places over three password-related help desk calls each year.
- The average cost-per-call ranges between \$25 and \$50.
- Absence of centralized administration requires multiple data sources to be updated and maintained independently.

Strategic Fit – User Considerations

Convenience and Ease of Use

- Users are typically required to remember multiple passwords.
- Passwords that are easy to remember compromise good security.
- Users tend to re-use the same password for multiple systems, which compromises security.
- Good security practice dictates nonsense passwords, unique passwords and frequent changes – which are hard to remember, so end users write them down, thus compromising security.
- Frequent calls to the help desk for password resets add to both end user dissatisfaction and high management costs.

Portability

- Passwords work anywhere.

Multi-purpose

- Passwords have only a single purpose.

Strategic Fit – Corporate Considerations

Relative Strength

- Very weak form of security.
- Easily guessed.
- Prone to shoulder surfing.
- Easily detected as they traverse the network.
- User is not aware when a password is stolen.
- Passwords stored on the server are vulnerable to readily available password-cracking tools.
- Trojan horses installed on desktops can capture and deliver keystrokes to a hacker.
- Users tend to re-use the same password for multiple systems.
- Users write down their passwords and frequently lose the paper.
- No logging or reporting functionality is provided; therefore there is no user accountability.
- No centralized administration. Passwords are vulnerable to security holes as new devices, applications and communication methods are added and users are added, deleted or change roles.
- No “roles based” access capability.

Robustness and Scalability

- Does not provide for replication.
- Does not provide fail-over capability.
- No imbedded disaster recovery.
- No centralized administration capability.

Interoperability and Integration

- Requires password management for each resource protected.

Future Flexibility

- No accommodation for future use of smart cards or other stronger forms of authentication.
- No support for future use of electronic signature.

Appendix B – RSA SecurID Hardware Tokens

Total Cost of Ownership Considerations

Acquisition Cost

- More expensive than passwords.
- Less expensive than smart cards (which include additional cost for required card readers and middleware).
- Less expensive than biometric devices (which include additional cost for required devices and enabling software).

Deployment Cost

- Requires distribution of the hardware token only – there is no need to deploy software, drivers, readers or cables.
- Lower deployment costs than solutions with client-side software (such as smart cards or biometrics) that must be deployed on every end user desktop.
- RSA Authentication Deployment Manager (bundled at no extra charge with RSA Authentication Manager Enterprise Edition) can significantly lower cost of deployment.

Cost of Management

- Reduced password-related help desk calls can significantly lower ongoing operating costs compared to passwords.
- Centralized administration in RSA Authentication Manager software eliminates the need to manage multiple data stores.

Strategic Fit – User Considerations

Convenience and Ease of Use

- Users authenticate based on something they know – a PIN – and something they have – the constantly changing code on a hardware token.
- The token passcode eliminates the need for users to remember multiple passwords.
- Easy to use – just enter the displayed code.
- Most end users are already familiar with the concept of the combination of a PIN and a changing passcode on a token.
- "Always on" device.

Portability

- Works anywhere – “zero foot-print” solution.
- Small size – fits in a pocket and can be attached to a key chain.

Multi-purpose

- Single function – generates a new passcode every 60 seconds.
- A single hardware token can serve as the means of access for multiple resources.

Strategic Fit – Corporate Considerations

Relative Strength

- Two-factor authentication results in a very strong form of security.
- Passcodes are generated dynamically and are less vulnerable to cracking tools.
- The passcode changes every 60 seconds, eliminating the threat of visual theft of passcodes and Trojan horse threats.
- Passcodes cannot be guessed or predicted.
- Users are aware when a token is stolen or lost.
- Network transmission of token codes cannot be easily detected.
- 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 or deleted or change roles.
- The token enables role-based access control.

Robustness and Scalability

- Replication, failover capability and disaster recovery features ensure high availability.
- 1 Master and up to 10 Replicas per Realm, for up to 6 Realms.
- RSA Authentication Manager is engineered to scale to hundreds of thousands of users.

Interoperability and Integration

- Interoperable with over 300 certified applications and products from over 200 Partners.
- Unlike competitive partner programs, RSA Secured® SecurID Ready partner products undergo extensive testing and documentation before being certified.

Future Flexibility

- RSA SecurID authentication has added value over many years across constantly evolving technologies, from dial-up to web to VPNs and WLANs.
- RSA Secured SecurID Ready partner program helps ensure continued access to new solutions.

Appendix C – RSA SecurID Software Tokens

Total Cost of Ownership Considerations

Acquisition Cost

- More expensive than passwords.
- Less expensive than hardware tokens.
- Less expensive than biometric devices (which include additional cost for required devices and software).

Deployment Cost

- Requires installation of the RSA SecurID Software Token application software and token seed record(s) onto client platform. No hardware deployment necessary.
- Lower deployment costs than solutions requiring the use of device drives (such as smart cards or biometrics).
- Web-based downloadable applications enable deployment of client-side software without touching every end user system.
- RSA Authentication Deployment Manager (bundled with RSA Authentication Manager Enterprise Edition license) can significantly lower deployment costs.

Cost of Management

- Reduced password-related help desk calls can significantly lower ongoing costs.
- Centralized administration in RSA Authentication Manager software eliminates the need to manage multiple data stores.

Strategic Fit – User Considerations

Convenience and Ease of Use

- The token passcode eliminates the need for users to remember multiple passwords.
- Easy to use – just enter the displayed code.
- Most end users are already familiar with the concept of the combination of a PIN and a token passcode.
- Designed for easy integration with other client applications, allowing a seamless extra layer of security on client workstations or other trusted computing devices.

Portability

- RSA SecurID Software token versions for Windows® Mobile, Palm and BlackBerry PDAs and for Mobile Phones enable secure access from anywhere at anytime.
- RSA SecurID token for Windows desktops and the RSA SecurID Toolbar token enable secure access from desktop and laptop computers.

Multi-purpose

- RSA SecurID software tokens perform a single function – generating token codes every 60 seconds.
- RSA SecurID software tokens are designed to work on host devices that perform multiple functions, such as PCs, PDAs and smart phones.
- RSA SecurID software tokens are now embedded onto USB storage devices from multiple manufacturers to enable a single device for data storage and secure access.

Strategic Fit – Corporate Considerations

Relative Strength

- Two-factor authentication results in very strong form of security.
- PINPad operation encrypts a PIN together with the token code, minimizing threats from keyboard or network sniffing.
- Passcodes are generated dynamically and are less vulnerable to cracking tools.
- Passcode changes every 60 seconds, eliminating the threat of visual theft of passcodes and Trojan horse threats.
- Randomly generated token codes cannot be guessed or predicted.
- Network transmission of token codes cannot be easily detected.
- 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.
- Software tokens support "roles-based" access control.

Robustness and Scalability

- Replication, fail-over capability and disaster recovery features ensure high availability.
- Authentication Manager software is designed to scale to hundreds of thousands of users

Interoperability and Integration

- SDK available for custom application integration.
- Login Automation function automates dialer-based remote access.
- PC version offers silent migration to facilitate version upgrades.
- Interoperable with over 300 certified applications and products from over 200 Partners.
- Unlike some competitive partner programs, RSA Secured SecurID Ready Partner products undergo extensive testing and documentation before being certified.

Future Flexibility

- RSA SecurID software token products are steadily expanding to cover the increasing variations of portable devices.
- RSA is working with device vendors to embed or bundle software into host platforms to enable native RSA SecurID operations.
- SecurID software token seed provisioning via RSA Authentication Deployment Manager saves time and increases convenience for setting up tokens on host systems.
- SecurID authentication has evolved from dial-up to web to VPN to Wireless LAN access.
- RSA Secured SecurID Ready partner program helps ensure continued access to new solutions.

Appendix D – RSA Digital Certificates

Total Cost of Ownership Considerations

Acquisition Cost

- Per user costs start at a high of \$30 per user for a low volume of users.
- The only renewal cost is maintenance (excluding web SSL certificates).

Deployment Cost

- An easy-to-use enrollment process minimizes the burden of deployment for information technology administrators.
- Web-based deployment of certificates is designed to enable quick, easy and cost efficient deployment.
- Deployment on smart cards requires the global deployment of smart card readers as peripherals.
- Deployment on USB devices requires no deployment of additional peripherals.

Cost of Management

- Suspension and revocation of digital certificates is easily and centrally controlled. This means that digital certificates can be managed without physically accessing them.
- Real-time Online Certificate Status Protocol ensures instant certificate status checking.

Strategic Fit – User Considerations

Convenience and Ease of Use

- RSA Digital Certificates are engineered to make enrollment very easy.
- Application integration enables virtual, transparent use of certificates from the end user's perspective.
- Use of digital certificates on smart cards or USB devices requires deployment of middleware.

Portability

- Digital certificates stored in the browser restrict the use of these credentials to the desktop/laptop.
- Digital certificates stored in smart cards enable secure access from networked locations with smart card readers.
- Digital certificates stored in USB devices enable secure access from PCs without the need for external peripherals.

Multi-purpose

- Digital certificates enable strong authentication across a wide range of applications – including: web applications, e-mail, VPNs and client/server applications.
- In addition to authentication, digital certificates serve other e-business functions such as ensuring data and transaction integrity, enabling digital signing and providing support for non-repudiation.
- Digital certificates on smart cards enable physical access to buildings and logical access to applications.

Strategic Fit – Corporate Considerations

Relative Strength

- Digital certificates can be "locked down" within the browser so they cannot be exported and are pass-phrase protected.
- Digital certificates provide strong protection against brute force attack with high encryption strength.

Robustness and Scalability

- RSA Certificate Manager has been independently tested to scale to over eight million certificates per Certificate Authority instance.
- One real-life example is of a customer who purchased RSA Certificate Manager and deployed 100,000 certificates within two months.

Interoperability and Integration

- RSA Certificate Manager-issued digital certificates are based on industry standards for wide scale interoperability.
- Leading vendors of VPNs, e-mail and a variety of web-based applications have inherent support for digital certificates.
- RSA offers RSA BSAFE toolkits to help organizations become certificate-aware regarding their legacy-based or custom-developed applications.

Future Flexibility

- Extensible nature of digital certificates ensures future flexibility and investment protection for customers.
- Uses include: web-based, client/server and device strong authentication.
- Application uses include: digital signing for online forms and documents, secure e-mail and others.

Appendix E – Hybrid One-time Password USB Tokens

Total Cost of Ownership Considerations

Acquisition Cost

- More expensive than smart cards or single-function hardware tokens.

Deployment Cost

- Requires issuance of hardware token and client software.
- Easy deployment of digital certificates to chip co-resident on the device.

Cost of Management

- Automated client software update process.
- Intuitive, web-based certificate configuration and administration.
- Centralized administration in RSA Authentication Manager eliminates the need to manage multiple data stores.

Strategic Fit – User Considerations

Convenience and Ease of Use

- Easy certificate enrollment with RSA Registration Manager auto enrollment.
- Minimal user interaction with the digital certificate.
- Digital certificates on smart USB devices support single sign-on.
- Auto-fill capability for OTP code eases use.

Portability

- Small size, fits in a pocket and can be attached to a key chain.
- OTP display enables remote access from anywhere, anytime.

Multi-purpose

- Can contain digital certificates that enable strong authentication across a wide range of applications, including web applications, e-mail, VPNs and client/server applications.
- In addition to authentication, digital certificates serve other e-business functions such as ensuring data and transaction integrity, enabling digital signing and providing support for non-repudiation.
- OTP functionality enables anywhere, anytime access.

Strategic Fit – Corporate Considerations

Relative Strength – OTP

- Two-factor authentication results in a very strong form of security.
- Passcodes are generated dynamically and are not vulnerable to cracking tools.
- Passcodes change every 60 seconds, eliminating the threat of visual theft of passcodes and Trojan horse threats.
- Randomly generated token codes cannot be guessed or predicted.
- Network transmission of token codes cannot be easily detected.
- RSA Authentication Manager 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" access control.

Relative Strength – Smart Card

- Embedded smart chips ensure high security for digital certificate and private key storage.
- Real-time certificate status checking with Online Certificate Status Protocol.
- Certificate authority root keys stored in bundled FIPS 140-1 Level 1-3 compliant HSM.
- Secure, web-based administration and certificate issuance through the RSA Digital Certificate Authority.
- Common criteria validated at EAL-4 level.

Robustness and Scalability – OTP

- Replication, failover capability and disaster recovery features ensure high availability.
- 1 Master and up to 10 Replicas per Realm, for up to 6 Realms.
- RSA Authentication Manager easily scales to hundreds of thousands of users.

Robustness and Scalability – Smart Card

- Independently tested to scale to eight million users for a single certificate authority deployment.
- Designed to maintain performance when scaled, supporting massive demand for signing operations, PKI queries and large-scale certificate storage and management.
- Also supports the geographic distribution of many Registration Authorities with multiple administrators.
- Customer can mirror their organizational structure by setting up any number of certificate authorities and administrators.
- Comprehensive backup and replication system for credentials.

Future Flexibility – OTP

- Can be used to provide secure access to digital certificates.
- RSA SecurID has added value over many years across constantly evolving technologies, from dial-up to web to VPNs to WLANs.
- RSA Secured Partner program ensures continued access to new solutions.

Future Flexibility – Smart Card

- Digital certificate use can be extended to include secure e-mail, e-forms, VPNs and web access.
- Smart card use can be extended to include secure logical access, physical access, picture ID and e-wallet.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance. RSA offers industry-leading solutions in identity assurance and access control, encryption and key management, compliance and 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.

RSA, SecurID and the RSA logo are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2006-2007 RSA Security Inc. All rights reserved.

ASC WP 0307



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC