



RSA SecurID Certified Systems Engineer Certification Examination Study Guide

Introduction

The RSA SecurID Certified Systems Engineer (CSE) examination is based on the critical job functions that an individual would typically be expected to perform with competence when working with the RSA SecurID product and RSA Authentication Manager software.

A Systems Engineer is a person who works in a technical support, sales support and/or technical implementation role within RSA, The Security Division of EMC, within an RSA reseller organization, or within an organization using RSA SecurID products.

An analysis of the major job functions expected of an RSA SecurID CSE determined that there are four major areas of job role responsibility:

- General knowledge about RSA SecurID technology and RSA Authentication Manager product capability
- Designing solutions incorporating RSA SecurID components from understanding an organization's needs and environments
- Installing solutions to meet requirements and which demonstrate RSA SecurID product functionality
- Supporting solutions through troubleshooting specific implementation and system integration issues

Candidate Background and Experience

A Certified Systems Engineer candidate should have a minimum of two years of professional experience in one or more of the following technical areas and understand how these technologies relate to and integrate with the RSA SecurID product. Elements of the CSE exam touch upon each of these areas.

- Remote Network Access
- Web Servers and Servlet support
- LDAP Directory Servers
- Internet and Networking Protocols
- Network and Network Security Applications
 - *Operating System (UNIX, Linux, Windows) security*
 - *Desktop and Workstation security*
 - *TACACS and RADIUS protocols*

Examination Domains

The RSA SecurID Certified Systems Engineer examination is comprised of four major Domains (subject areas). Each Domain is represented by a series of questions designed to evaluate competence and knowledge of elements relating to that domain. The following table describes the proportion of the examination that relates to each domain:

Domain	% of Examination
1.0: RSA SecurID Product Knowledge	40 %
2.0: Assessment / Design Solution	30 %
3.0: Install Solution	20 %
4.0: Support	10 %
TOTAL	100 %

Domain 1.0: RSA SecurID Product Knowledge

The Certified Systems Engineer must have a fundamental knowledge of key features and benefits of the RSA SecurID product family. The CSE is expected to be able to identify business solutions that highlight the product features and benefits within customer environments and demonstrate how the product solves important issues.

Content Areas

- Competitive Analysis
 - *Technology Strengths*
 - *Interoperability (RSA SecurID Ready and RSA Secured products and components)*
- RSA Authentication Manager technology and functionality
- Industry Technology
 - *Authentication philosophy and concepts*
- RSA Product Family
- Features and Functions
 - *RSA Authentication Manager*
 - *RSA Authentication Agents*
 - *RSA SecurID Appliance*

Domain 1.0 Sample Items

When would configuring a Windows agent "Reserve Password" be advisable?

- If the agent is also a RADIUS server.
- If users have not yet been issued tokens.
- If the agent is used only for offline authentication.
- If the agent is configured to "Challenge All Users".

'D' is the correct choice because the Challenge All Users configuration can lock out all users – including the administrator – if communication between agent and server is interrupted. A Reserve Password can allow an administrator access to the agent machine.

An RSA SecurID SID800 token (also known as a "USB token")

- cannot be used with alpha-numeric PINs.
- must be connected to a computer USB port to generate tokencodes.
- allows users to communicate securely through directly connected USB devices.
- allows tokencodes to be read from a display and supplied programmatically through a USB port.

'D' is the correct choice. The SID800 allows both of the stated functions. Statements 'A', 'B', and 'C' are false – the SID800 token CAN be used with alpha-numeric PINs (if security and PIN policies allow), it does NOT require connection to a computer to generate codes, and it provides no functionality for communication via USB devices.

The amount of offline data downloaded to an agent is determined by

- the value set during agent installation.
- the value configured in the agent Security Center.
- the Authentication Manager Security Console offline authentication policy.
- the number of successful authentications made to the agent before going off line.

'C' is the correct choice – the offline authentication policy sets the number of days' of downloaded data to the agent. Statements 'A', 'B', and 'D' are false – offline data configurations are NOT made during installation or through the agent Security Center, the number of successful authentications have no influence on the amount of downloaded offline data.

Domain 1.0 Sample Items (continued)

To restrict user authentication by time of day,

- users must be members of a group.
- a user's token record must be configured.
- the individual user record must be configured.
- Agents must be configured for restricted times.

'A' is the correct choice because only User groups can be configured with time restrictions. The other choices are not correct statements.

Which of the following are pre-defined administrative roles in a default Authentication Manager deployment? (CHOOSE TWO)

- Site Administrator.
- User Administrator.
- Realm Administrator.
- Help Desk Administrator.

Choices 'C' and 'D' reflect administrative roles that exist in a default deployment. Choices 'A' and 'B' could be defined with these names by creating customized roles but they are not pre-defined in the system.

A user connects to a VPN entering their RSA SecurID username and PASSCODE. The user is prompted to wait until the code on the token changes, then to enter the next code. What has occurred?

- The user is in Next Tokencode mode.
- The Server is too busy to respond to requests at the moment.
- A VPN connection is delayed one minute for security purposes.
- The code on the token has already been used for a previous authentication.

'A' is the correct choice – Next Tokencode mode involves such a user prompt. Statements 'B', 'C', and 'D' are false.

If an RSA SecurID Appliance model 250 is installed as a Primary server, a Replica server can be installed in the deployment using either a model 130 Appliance, model 250 Appliance, or RSA Authentication Manager software.

- True
- False

This statement is false. Mixing Appliances and Authentication Manager software within a single deployment is not supported. Either all-Appliance or all-software solutions must be used.

On-Demand tokencodes use UCT (GMT) time for calculating the tokencodes.

- True
- False

This statement is false. Unlike Time-synchronous tokens, On-Demand tokencodes are a single-use code generated by Authentication Manager and are not time dependent.

Domain 2.0: Assessment / Design Solution

The Certified Systems Engineer must be able to conduct an assessment of an organization's environment, an organization's business needs, and architecture. Based on this assessment, the CSE must be able to identify appropriate RSA SecurID solutions that will meet these needs.

Content Areas

Assessment

- How/Why does an organization plan to use the product
- What is the organization's long-term goal or need
- Security Policy and Security Assessment
- Interoperability with non-RSA SecurID components
- Architecture
 - *Desktops/Workstations*
 - *Operating Systems*
 - *Network*

Design

- Architecting for:
 - *Security*
 - *Scalability*
 - *Redundancy*
 - *Performance*
 - *RSA Authentication Agent applications*
 - *RSA SecurID Appliance applications*

Domain 2.0 Sample Items

Which of the following is an important factor in determining how RSA Authentication Agents are installed and configured?

- The licensed limit for Agents in a deployment
- An organization's security policy and access control plan
- The number of users linked to an external LDAP Identity Source
- Whether a deployment will contain multiple Realms or Security Domains

'B' is the correct choice. An organization's policies and plans determine where Agents are required and how they will be used (challenge all users, challenge some users, protect specific resources, etc.) 'A' is not correct because the license does not limit the number of Agents in a deployment; 'C' and 'D' are not factors in determining Agent installation or configuration.

The term 'SecurID Ready' indicates that

- the server authentication engine and activity log have both been started properly
- a user has passed a security screening and is now ready to use an RSA SecurID token
- an RSA SecurID token code has flashed three times and is ready to be entered at login
- an Agent product has been tested and certified to work with RSA Authentication Manager

'D' is the correct choice. The other choices have nothing to do with "SecurID Ready" products.

Domain 2.0 Sample Items (continued)

What would be the best strategy for an organization that wants to plan for installing Authentication Manager software or an RSA SecurID Appliance in their headquarters and disaster recovery facility sites?

- Locate both a Primary and Replica instance at the disaster recovery facility to assure safety in the event of a disaster at the headquarters site.
- Locate a Primary instance at the disaster recovery facility and a Replica instance at the headquarters site to assure administrative access in an emergency.
- Locate both a Primary and Replica instance at the headquarters site and a RADIUS Server at the disaster recovery facility to process authentications in an emergency.
- Locate a Primary instance at the headquarters site and a Replica instance at the disaster recovery facility to provide a server that can be promoted to Primary, if needed.

'D' is the best choice. The Primary instance at the headquarters site is most easily accessible for routine administration and the Replica instance can be promoted to a Primary in the event of a disaster (and is safely located at the disaster recovery facility).

'A' is not the best choice because the Primary instance would typically be more useful in closer proximity to where routine administration occurs. Also, if a disaster should strike the disaster recovery facility, the servers would not have alternative backups. 'B' is not a good choice because the Primary should be more accessible for routine operation.; 'C' is not a good choice because a RADIUS Server operating alone in a disaster recovery facility would need the services of a Primary or Replica server which might be unavailable if a disaster should strike the headquarters facility.

Which of the following functions is different in the RSA SecurID Appliance compared to the functions available with RSA Authentication Manager software?

- Only an Appliance can rollback software updates using the Operations Console.
- Only the Appliance can add and configure Authentication Agent records manually.
- Only Authentication Manager software can allow additional Identity Sources to be defined.
- Only Authentication Manager software can allow the Primary server hostname to be specified during initial setup and installation.

'A' is the correct choice. The Operations Console of the RSA SecurID Appliance allows control over both applying and rolling back software updates. 'B', 'C', and 'D' are not correct because all of the functions described can be performed both in a software deployment as well as an appliance deployment.

Of the following choices, what criteria would typically dictate how RSA Authentication Agents are deployed?

- The licensed limit for Agents in a deployment
- An organization's security policy and access control plan
- The number of users linked to an external LDAP Identity Source
- Whether a deployment will contain multiple Realms or Security Domains

'B' is the correct choice. An organization's policies and plans determine where Agents are required and how they will be used (challenge all users, challenge some users, protect specific resources, etc.) 'A' is not correct because the license does not limit the number of Agents in a deployment; 'C' and 'D' are not factors in determining Agent installation or configuration.

If an organization has a mix of operating systems (for example, Windows 2003, Solaris and Linux) Authentication Agent to Authentication Server communication is supported between these platforms.

- True
- False

This statement is true. Agent-to-Server communication can take place between different OS platforms.

Domain 3.0: Install Solution

The Certified Systems Engineer installs a solution appropriate to an organization's environment. The CSE must be able to identify the procedures and configuration issues for installing an RSA SecurID system or systems and bringing the software to an appropriate operational level to meet the organization's requirements. In addition, the CSE must know how to develop a controlled rollout to end-users, assess end-user acceptance, and provide pre-deployment information and education.

Content Areas

- Installation
 - *Platform, Hardware, and Operating Systems*
 - *RSA SecurID Appliance setup*
- Configuration
 - *User, Group, Site Structures*
 - *Agent and Agent host configurations*
 - *Tokens: types, differences between types, and deployment strategies*
 - *RADIUS/TACACS*
 - *Interoperability with non-RSA SecurID components*
- Integration
 - *Client (Agent)*
 - *Third-Party (non-RSA SecurID) components*
 - *Redundancy/Scalability*
 - *Connectivity*
- Documentation
 - *Skills Transfer*
- Testing (QA)
 - *Agent authentication*
 - *Third-party authentication*

Domain 3.0 Sample Items

If a firewall separates an Authentication Agent and Authentication Manager server, ports 1024-65535 should be opened for UDP communication?

- True
 False

This statement is true. For the Server to Communicate to the Agent through a firewall, the port the Agent uses as its source port for an authentication request must be open from the Primary and Replica(s) IPs to the Agent IP. This port can be any port from 1024 to 65535/UDP (the Agent simply requests a port from the operating system).

When is creation of an Authentication Manager "Package" file necessary? (CHOOSE TWO)

- When installing or configuring a Primary database server
 When installing a Replica server to Authentication Manager software
 When installing an Authentication Agent to an RSA SecurID Appliance
 When installing an add-on RSA RADIUS server to Authentication Manager software

'B' and 'D' are the correct choices – creation of a package file from the Primary server is necessary for each of these installations. Choice 'A' is not correct – a package is not necessary for the Primary Database Server installation (the Package file originates at the Primary server); Choice 'C' is not correct – a package is not necessary for Agent installation.

Domain 3.0 Sample Items (continued)

What does an Agent "Alternate IP Address" allow?

- It allows the Agent to send authentication requests to multiple Servers.
- It allows the Server to recognize authentication requests from an agent either directly or through address translation.
- It allows alternate encrypted communication channels between Agent and Server for PIN setting and Next Tokencode modes.
- It allows alternate encrypted communication channels between Agent and Server for downloading offline authentication "day files".

'B' is the correct choice – the Alternate IP Address setting adds one or more IP addresses to an Agent record to accommodate network address translation through firewalls and routers or when accommodating multi-homed Agent hosts. Choices 'A', 'C', and 'D' are false.

For an RSA Authentication Agent for PAM (Pluggable Authentication Module), which of the following statements is true?

- Users must have 'sdshell' designated as their default shell.
- Service, Rule, and Module information is designated in the pam.conf file
- RSA SecurID users authenticating to the PAM agent must have root privileges.
- To enable PAM authentication, the OS services file must contain a SECURID_PAM TCP service entry.

'B' is the correct choice – the pam.conf file contains the necessary configuration information for designating user authentication. Choices 'A', 'C', and 'D' are false statements.

If a RADIUS server is **NOT** installed at the same time as a Primary Authentication Manager [software] server,

- It cannot be installed within the same deployment.
- It can be installed on a different host machine at a later time.
- It can be installed on the Primary host at a later time by running the installer program.
- It can be added by using the configuration options in the Authentication Manager Operations Console.

'B' is the correct choice. A RADIUS server cannot be added to an installed Primary server but it can be installed on a separate host machine. (the Primary server can also be uninstalled, then re-installed with the RADIUS option, if desired). 'A' is not correct because the RADIUS server can be installed as stated above. 'C' is not correct – RADIUS cannot be added by simply re-running the installer. 'D' is not correct because RADIUS cannot be added using the Operations Console.

When an RSA Authentication Agent for Microsoft Windows is installed on a workstation in a Windows domain environment,

- an "aceInt.dll" file is added to the \system32\ directory to handle user logon
- the Authentication Agent is automatically configured for offline authentication
- users must open the Agent Security Center to enable RSA SecurID authentication
- the Authentication Agent software must be installed on the Domain Controller as well

'A' is the correct choice. The 'aceInt.dll' replaces the function of the original 'msgina.dll' to handle user logon (the msgina.dll is not replaced – it remains on the host in case the Authentication Agent is uninstalled). 'B' is not correct because offline authentication is configured through the server Security Console and not during Agent installation. 'C' is not correct because users typically do not have access to the Security Console – it is accessible only by administrators. 'D' is not correct because the Agent on the workstation host will process authentication requests – an Agent on the Domain Controller is not required.

Domain 4.0: Support Solution

The Certified Systems Engineer needs to provide support and troubleshoot issues throughout the installation phases and after implementation.

Content Areas

Assessment

- Troubleshoot issues
 - *RSA Authentication Manager and System log interpretation*
 - *Problem reproducibility*
 - *Offline authentication problems*
- Communication with Technical Support
 - *Problem definition*
 - *Questioning/interrogation*
 - *Environment*
- Translation to Technical Support
 - *Problems, message logging and interpretation*

Domain 4.0 Sample Items

If users of time-synchronous tokens as well as users with 'fixed passcodes' are being denied access to authentication through a single server, a possible cause is that

- the server clock is mis-set by more than 20 minutes
- services are not running on the authentication server
- an SMS service has not been configured to deliver tokencodes
- the Microsoft Management Console snap-in was not properly configured

'B' is the correct choice given these four possibilities. 'A' is not correct because a mis-set server clock would affect time-synchronous tokens but not fixed passcodes, which do not have any time dependency. 'C' is not correct because an SMS service would deliver "On-Demand" tokencodes, not any other type of code. 'D' is not correct because the MMC snap-in would relate to token assignment and not authentication.

A "Business Continuity Option" (BCO) license is used for

- Increasing the capacity for active users in a deployment.
- extending the expiration date of a Base or Enterprise license.
- Adding multiple Replica servers to take over for a failed Primary server.
- Utilizing a NAS-based database to continue operations in case of catastrophic failure.

'A' is the correct choice. A BCO license allows an immediate increase in the number of users that can become active (assigned tokens or on-demand tokencodes) in the event of an emergency that forces a large number of users to work remotely. 'B', 'C' and 'D' are not correct – the Business Continuity Option does not offer such capability.

A configured logging level applies only to the instance in which it is configured.

- True
- False

This statement is true. Logging levels are utilized only within an instance and logging levels can be configured differently for Primary and Replica instances, if desired.

Domain 4.0 Sample Items (continued)

An Authentication Activity Monitor would show what type of events, by default?

- network failures
- user logout times
- authentication failures
- Agents that are on-line

'C' is the correct choice. None of the other types of events are displayed in the Authentication Activity Monitor.

A message of "Node secret mismatch" in a log report would probably indicate that (CHOOSE TWO)

- corruption of the Node Secret file has occurred
- Authentication Agent software was uninstalled then re-installed
- a user has incorrectly revealed a node secret value to an attacker
- the Authentication Manager database has been restored from a backup

'A' and 'B' are correct possibilities. If Agent software is uninstalled and re-installed, the Node Secret value is re-set to its default state and will not match the value in the Authentication Manager database. The same mismatch would occur if the Node Secret file was corrupted. 'C' is not correct because a user could not realistically reveal a node secret value to anyone (Strictly speaking, if a user were to copy and send a Node Secret file to an accomplice attacker, and the attacker attempted to use this file on a different Agent, a mismatch would result – but this scenario would require the counterfeit Agent to also be added to the Authentication Manager database) 'D' is not correct because a database restoration would not typically result in a mismatch (but, strictly speaking in this case, it might be possible for an old database backup to contain old, obsolete Node Secret information – but this is not the 'probable' case because a trained professional is very good at maintaining up-to-date system backups).

If a user enters their RSA SecurID passcode in reverse order (tokencode first, then PIN) what event message would probably appear in an Authentication Report.

- Authentication method failed
- Passcode format error
- Bad PIN, Good tokencode detected
- Authentication successful (system would interpret PIN and Tokencode correctly)

'A' is the correct choice. The system would not be able to determine what components of the supplied string were PIN and Tokencode (unless, by chance, the leading digits of the Tokencode were actually the user's PIN – in which case, the logged message indicate Good PIN, Bad tokencode) None of the other choices are correct.

General Topic Areas for Study and Relevant Experience

The following list provides suggestions for concentrating your study efforts for this exam and areas in which you will want to explore when working with the RSA SecurID product in your own environment.

General Product Knowledge

- What constitutes a PASSCODE in term of RSA SecurID two-factor authentication
- Licensing options in regard to users, features and functions (Business Continuity, Base vs Enterprise, Credential Manager, etc.); Authentication Manager response when a license is out of compliance or beyond allowed limits
- Basic operations and differences between token types – standard, PINPad, Software token, Event-based tokens, ON-Demand Tokencodes, USB tokens, etc.
- Differences between Authentication Manager structures – Replica and Primary servers, internal and external Identity Sources

Operations and Administrative Topics

- Authentication Manager configurations and administrative objects that can and cannot be shared and/or moved between Realms, Identity Sources, Security Domains and Groups (for example, a RADIUS server can only be associated with one Realm)
- Policy options for configuring user PINs, Passwords, Offline Authentication, etc.
- Structure and use of credential sets for different authentication purposes – RSA SecurID, access to self-service console, LDAP credentials, access to administrative consoles
- Default Authentication Manager administrative roles; capabilities to create new or customized roles
- Types and functions of logging and monitoring capabilities – Activity monitors, logging options; creating and customizing system, data, and activity reports.

Solution Design Topics

- Configuration limits such as number of allowed tokens per user, servers per instance, instances per deployment, etc.
- Authentication Manager installation options (stand-alone database, RADIUS server options, Replica instance) and failover options and configurations for these servers
- Basic operations and differences between token types – standard, PINPad, Software token, Event-based tokens, On-Demand Tokencodes, USB tokens, etc.
- Relationship of an organization's security policy to Authentication Manager installation and configuration – including server placement, disaster recovery, Agent deployment, and user policies (password/PIN structure, lockout policy, etc.)
- Communication paths and protocols between Agents and servers; firewall and router accommodations; port usage

Installation and Configuration Topics

- How Agents such as Remote Access Server (RAS) and Pluggable Authentication Module (PAM) are configured for authentication – e.g. where Agent software is needed, what system files are used
- Configuration for on-line and offline functionality, emergency access codes, and Windows password integration; configurations for Agent-to-server load balancing
- Installation procedures for Primary server instances, Replica server instances, RADIUS servers, and Agents; command line utilities available to test communication, re-balance server lists, create data backups, etc
- Installation, configuration and use of the Microsoft Management Console (MMC) snap-in
- Setup and configuration of log archive signing
- General pre-installation requirements and preparation for installation on Windows, UNIX and Linux platforms

Examination Preparation

Product Training

Although RSA SecurID product training is not a strict requirement in preparation for the RSA SecurID Certified Systems Engineer Certification Examination, it is highly recommended. Analysis of test results indicates that a majority of candidates who attend RSA SecurID training prior to testing are more likely to successfully pass the exam on their first attempt.

RSA Security offers the following courses that relate to the RSA SecurID product and material covered on the CSE exam:

- RSA SecurID Administration
 - *This course covers the fundamental concepts and operating principles of RSA SecurID technology; end-user organization and administration; system functions; end-user support.*
- RSA SecurID Installation and Configuration
 - *Assumes prerequisite experience of RSA SecurID Administration. This course covers installation and configuration of RSA SecurID system components; deployment planning; strategies for system redundancy and load-balancing.*
- RSA SecurID Product Fundamentals
 - *This course covers a number of the topics of the Administration and Installation and Configuration courses described above – which comprises the essential information identified for systems and sales engineers. This course is only available to RSA SecurWorld channel resale partners.*

For full and detailed descriptions of RSA Security course offerings, visit: www.rsa.com (use the [Services > Training and Certification](#) links).

Product Experience

Many of the areas addressed by the CSE exam will be familiar to the candidate who has worked with the RSA SecurID product through installation and configuration of RSA Authentication Manager, Agents, and other components and through familiarity with administrative operations.

For example: Knowing what reporting capabilities exist in RSA Authentication Manager speaks to the candidate's overall product knowledge; Understanding how Authentication Manager Realms and Security Domains are structured speaks to the candidate's ability to set up an extensible security solution.

The CSE exam content areas cover a wide range of RSA SecurID product capability because a Certified Systems Engineer may be called upon to install or deploy an RSA SecurID solution for a variety of requirements or scenarios. A candidate who has worked for a long period in one organization (under that organization's specific deployment scheme) may not have a particular advantage over a candidate who has worked for a shorter period of time installing a variety of solutions for a number of organizations. Therefore, it is difficult to quantify a time period of relevant product experience. The general recommendation is that the candidate should actively work with the RSA SecurID product and components for 3 to 6 months prior to taking the exam – in addition to other preparation.

It is important to note that The CSE exam contains a mix of topics that relate to administrative operations as well as system design/installation. A candidate who has simply installed an RSA SecurID deployment without having direct experience with RSA Authentication Manager administrative operations will probably not have sufficient experience to answer a majority of the administrative items on the exam. Knowledge transfer on administrative matters to customers and users as well as the ability to thoroughly demonstrate and prove operation concepts is considered part of a CSE's realm of expertise.

Study and Preparation Materials

As is common with other industry certification exams, RSA SecurID CSE examination questions were constructed, reviewed, edited, and refined by groups of subject matter experts. A requirement of each test item is that it be referenced to a definitive source – document, publication, product menu selection, etc. Therefore, a finite set of preparation materials can be recommended for study and exam preparation. Although not all of the materials listed below are available in the public domain, the list does constitute a body of knowledge from which examination test items have been drawn.

- RSA Security Training Materials (Available only as part of an RSA Security training program)
 - *RSA SecurID Administration Course Student Guide*
 - *RSA SecurID Installation and Configuration Course Student Guide*
 - *RSA SecurID Product Fundamentals Course Student Guide*
- RSA SecurID product documentation (Available with the product software)
 - *RSA Authentication Manager Administrator's Guide*
 - *RSA Authentication Manager Installation Guide*
 - *RSA Authentication Manager Planning Guide*
 - *Authenticating with RSA SecurID (end-user instructions)*
 - *RSA Authentication Agent Installation and Administration Guides*
 - *RSA Authentication Manager and RSA Authentication Agent README documents*
- RSA Authentication Manager Help Menus and Help Screens (These Help functions are only available as part of installed and operating RSA Authentication Manager software. RSA Authentication Manager may be available to you as a qualified trial evaluation through the RSA Sales organization. To apply for a trial evaluation if you do not already own the RSA Authentication Manager product, visit the RSA web site.)

Examination Details

Testing Centers, Locations, and Registration

The RSA SecurID Certified Systems Engineer examination is administered by the Pearson VUE organization – an internationally known examination provider. Examination centers are located worldwide. Visit the Pearson VUE web site (www.vue.com) and use the [Test Center Locator](#) to find a testing facility convenient to you.

You may also use the Pearson VUE site to create a personal login account and register for an exam. The RSA SecurID Certified Systems Engineer exam code is 050-v71x-CSESECURID (this exam reflects experience with RSA Authentication Manager version 7.1 software)

Exam Questions

The RSA SecurID CSE exam consists of 71 questions to be completed in 90 minutes. The exam consists of multiple-choice, multiple-response, or true/false type questions. The exam is computer-based and closed book – you may not utilize any printed material, personal computers, calculators, cell phones, etc. during the test.

The minimum passing score is 70%. Test results are calculated automatically at the conclusion of the test and testing center personnel can provide you with an authorized copy of your results before you leave the testing center.

Exam Costs

The fee for taking the exam is US\$ 150.00.

Language Availability

The RSA SecurID Certified Systems Engineer exam is available in English.

What to expect at the Testing Center

You must present two forms of identification; one of which is a photo ID.

You will be required to electronically accept the terms of an RSA Certified Security Professional Certification Non-Disclosure and Program Agreement before beginning the examination.

Re-taking the Exam

There is no limit on the number of times that you can re-take the certification exam. However, to maintain integrity and confidentiality of the test items, 60 days is the required elapsed time before retaking the test a third time. Please note that you must pay the full exam fee each time that you retake the test.