



RSA Digital Certificate Management Solutions Certified Systems Engineer Certification Examination Study Guide

Introduction

The RSA Digital Certificate Management Solutions 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 Certificate Management product and components. The components include: RSA Certificate Manager, RSA Registration Manager, RSA OneStep, RSA Key Recovery Manager, and RSA Certificate Manager API.

A Systems Engineer is a person who works in a technical support, sales support and/or technical implementation role within RSA Security, within an RSA Security Reseller organization, or within an organization using RSA Digital Certificate Management Solutions products and technology.

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

- General knowledge about the technology, product capability, PKI concepts, and PKI-related industry standards involved with the RSA Digital Certificate Management Solutions product
- Designing solutions from understanding an organization's needs and environments – applying PKI and digital certificate technology as required
- Installing solutions to meet requirements and which demonstrate digital certificate 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 product suite. Elements of the CSE exam touch upon each of these areas.

- Web Server and Browser implementation and support
- LDAP Directory Server architecture and implementation
- Internet and Networking Protocols
- PKI concepts relating to Digital Certificates, Public/private key technology, and industry standards
- General Network, Operating System, and Network Security principles and applications

Examination Domains

The RSA Digital Certificate Management Solutions (DCMS) 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 DCMS Product Knowledge	40 %
2.0: Assessment / Design Solution	30 %
3.0: Install Solution	20 %
4.0: Support	10 %
TOTAL	100 %

Domain 1.0: RSA Digital Certificate Management Solutions Product Knowledge

The Certified Systems Engineer must have a fundamental knowledge of key features and benefits of the RSA Digital Certificate Management Solutions product. 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

- RSA Digital Certificate Management Solutions product functions, capabilities and architecture
 - *Components and methodology (CRL publishing, CA and Jurisdiction configurations, etc.)*
 - *Applications (VPN, S/MIME, browser support, etc.)*
- RSA Digital Certificate Management Solutions Components (CA, RA, Key Recovery, OneStep)
- Industry Technology and Standards
 - *X.509, PKCS standards*

Domain 1.0 Sample Items

Which of the following is **NOT** a value of using an RSA Registration Manager (RM)?

- The RM performs local signing operations.
- Use of an RM allows end user enrollment within the DMZ.
- Vettor operations can take place closer to end users in an RM.
- RMs can be distributed across a wide geographical area to improve end user access.

'A' is the correct choice because all of the other statements are legitimate values of using an RM.

*Choice 'A': The RM does **not** perform signing operations (this function is reserved for the CA).*

Choice 'B': An RM server may be placed in the DMZ for access by end users for enrollment while securing the valuable CA resource behind a firewall.

Choice 'C': Distributed RMs allow vetting to occur on a local or regional level.

Choice 'D': Geographical distribution for local access is one reason RAs are employed.

RSA Certificate Manager jurisdictions

- require Jurisdiction Vectors for each jurisdiction.
- require Jurisdiction Administrators for each jurisdiction.
- help to segment an end-entity population into logical groups.
- conform to the PKCS #11 standard for cryptographic token sharing across domains

'C' is the correct choice because jurisdictions are designed to help structure a population into organizational, geographic, or other logical segments.

Choices 'A' and 'B' are not correct because separate Vectors and/or Administrators for each jurisdiction are not required.

Choice 'D': Although PKCS #11 does relate to cryptographic tokens, Certificate Manager Jurisdictions and use of tokens across domains is unrelated.

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 digital certificate solutions that will meet these needs.

Content Areas

Assessment

- How/Why does an organization plan to use PKI and PKI components
- What is the organization's long-term goal or need
- General security assessment
- Interoperability with non-RSA components
- Security Policy
- Architecture design
 - *Desktops/Workstations*
 - *Operating Systems*
 - *Network security, scalability, redundancy, performance*

Domain 2.0 Sample Items

A worldwide organization has a large number of users in an LDAP database. Any user existing in the database may receive a digital certificate to access the organization's secure web resources. The turnaround time to vet a certificate request is now twenty-four hours and the organization would like to reduce this time without hiring additional administrative personnel. What suggestion would help this organization?

- Implement RSA OneStep to automatically process certificate requests.
- Establish a jurisdiction for all users in the database to reduce the vetting period.
- Add RSA Registration Authorities (RAs) to distribute requests over several vendors.
- Implement RSA Access Manager to add protection to the existing web resources.

Choice 'A' is correct. Choice 'B' will not reduce the vetting period; Choice 'C' does not achieve the personnel objective of the organization; Choice 'D' will have no effect on the stated problem.

If an organization is concerned about secure, emergency access to encryption keys, which of the following might be recommended?

- A Hardware Security Module with 'M of N' operators configured.
- A Hardware Security Module with one trusted Key Administrator configured.
- RSA OneStep and SSL protection of a private key store.
- Configuring the RSA Certificate Manager Administration Console for access by 'M of N' operators.

'A' is the correct choice.

Choice 'B' is not a secure solution because key access is left to a single individual.

Choice 'C' and 'D': These are not valid options for protection of encryption keys.

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 Digital Certificate Management 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*
- Configuration
 - *CA, RA, and Jurisdiction Structures*
 - *Location and types of system configuration files; configuration options*
 - *CA certificate extension profile configurations and options*
- Integration
 - *Establishing inter-CA trust relationships*
 - *PKI object publication and importation*
- Component interoperation
 - *RSA Registration Manager RA synchronization*
 - *RSA OneStep installation and configuration*

Domain 3.0 Sample Items

In what ways can the RSA Certificate Manager be configured for CRL publication (CHOOSE THREE)?

- Locally through HTTP
- Locally through LDAP
- Locally through OCSP
- Externally through HTTP
- Externally through LDAP
- Externally through OCSP

Choices 'A', 'B', and 'E' are correct. Both local and external LDAP publication are supported as well as publication through the local HTTP server. None of the other choices are valid options (OCSP responds to validity requests but does not publish a CRL).

Which of the following is a valid statement in regard to an RSA Registration Manager installation?

- The CA Operations workbench is only available to registration Registration manager Vectors.
- The CA Operations workbench is only available to Registration Manager Administrators.
- The Registration Manager can employ several Vectors and enroll users only in a single Jurisdiction.
- The Registration Manager can employ only a single Vettor and enroll users in several Jurisdictions.

Choice 'C' is correct – only one Jurisdiction is served by a Registration Manager but there may be several Vectors. Choice 'D' is incorrect because it states the opposite; Choices 'A' and 'B' both reference the CA Operations workbench that does not exist in an Registration Manager installation.

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 log file locations*
 - *RSA log file and System Log interpretation*
 - *Problem reproducibility*
- Communication with Technical Support
 - *Problem definition*
 - *Questioning/interrogation*
 - *Environment*
- Escalation process
 - *Escalation path*
- Translation to Technical Support
 - *Problems, message logging and interpretation*

Domain 4.0 Sample Items

Verifying and deleting log files

- are functions reserved for the Auditor
- can be performed by the Vettor and Administrator
- requires an 'M of N' number of Key Recovery Operators
- must use the private key of the System CA Administrator

Choice 'A' is correct.

Choice 'B' is not entirely correct – a Vettor cannot perform log verification and deletion operations (an Administrator may, if given Auditor priviledges).

Choice 'C': 'M of N' configurations and Key Recovery have nothing to do with log verification/deletion

Choice 'D': The private key of the System CA Administrator cannot, by itself, be used for log verification/deletion

Why might an application report that a certificate is invalid (CHOOSE THREE)?

- the certificate is expired or revoked
- a required extension value is missing from the certificate
- the approving Vettor is not authorized for that Jurisdiction
- the CA that issued the certificate is not trusted by the browser
- the certificate has not yet been posted to the CRL's "valid" list

Choices 'A', 'B' and 'D' are possible causes for an "invalid" message.

Choice 'C' is not applicable because without proper authority, a certificate would not have been vetted or issued in the first place.

Choice 'E': CRLs only contain information on invalid certificates – they do not have a "valid" list.

Examination Preparation

Product Training

Although RSA Digital Certificate Management Solutions product training is not a strict requirement in preparation for the Certified Systems Engineer Certification Examination, it is highly recommended.

RSA Security offers the following courses that relate to the RSA Digital Certificate Management Solutions product and material covered on the CSE exam:

- Cryptographic and Digital Certificate Concepts
 - *This course covers the fundamental concepts and principles of a PKI, Public/Private keys and encryption, and common PKI applications.*
- RSA Digital Certificate Management Solution Installation and Administration
 - *This course covers the installation and configuration of the RSA Digital Certificate Management Solutions product, system components, and deployment planning. It uses a case study structure to highlight the responsibilities and options available for all administrative and certificate management operations.*

For full and detailed descriptions of RSA Security course offerings, visit: www.rsasecurity.com/training/.

Although many of the topics that are part of the RSA Security product training courses may appear on the CSE examination, it is important to note that the focus of product training is to teach a student how to deploy and use the product effectively – it is not an examination preparation course, per se.

Product Experience

Many of the areas addressed by the CSE exam will be familiar to the candidate who has worked with, installed, and configured the RSA Digital Certificate Management Solutions product and its various components. Familiarity with administrative operations and troubleshooting also comes from direct experience with the product.

For example: Knowing what administrative roles can perform certain certificate management tasks speaks to the candidate's overall product knowledge; Understanding how the RSA Registration Manager interacts with the RSA Certificate Manager speaks to the candidate's ability to set up an extensible PKI solution.

The CSE exam content areas cover a wide range of RSA product capability because a Certified Systems Engineer may be called upon to install or deploy RSA Digital Certificate Management Solutions for a variety of requirements or solution 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 product and components for 3 to 6 months prior to taking the exam – in addition to other preparation.

Study and Preparation Materials

As is common with other industry certification exams, RSA 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 Security Cryptographic and Digital Certificate Concepts Student Guide*
 - *RSA Digital Certificate Management Solution Installation and Administration Student Guide*
- RSA product documentation (Available on the product software CDs and from RSA Security SecurCare On-Line for RSA Security customers with maintenance contracts. Some of these documents are also available for on-line, print-on-demand purchase by visiting www.rsasecurity.com/go/documentation.)
 - *RSA Certificate Manager Administrator's Guide*
 - *RSA Certificate Manager Installation Guide*
 - *RSA Registration Manager Administrator's Guide*
 - *RSA Registration Manager Installation Guide*
 - *RSA OneStep Developers Guide*
 - *RSA Key Recovery Manager Administrator's Guide*
 - *API Reference Manual*
- RSA Certificate Manager administration console Help Menus and Help Screens (These Help functions are only available as part of an installed and operating RSA Certificate Manager.
- Industry Standards literature, publications, and RFCs such as:
 - *Introduction to the PKCS Standards (RSA Security / RSA Laboratories)*
 - *ITU-T(International Telecommunications Union / ITU Telecommunication Standardization Sector) Recommendation X.509*
 - *Network Working Group RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)*
 - *IETF (Internet Engineering Task Force) IP Security Protocol (IPSec) working group drafts and related RFCs*

Books and publications

Although the majority of examination questions will **not** be drawn or referenced directly from the publications listed below, a general knowledge and awareness of PKI, Digital Certificate technology, and Information Security may be helpful to implicitly interpret some examination questions.

“Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves”

authored by: Randall K. Nichols, Daniel J. Ryan, and Julie J.C.H. Ryan

published by: RSA Press and McGraw-Hill

ISBN: 0072122854

“PKI: Implementing and Managing E-Security”

authored by: Andrew Nash, William Duane, Celia Joseph, and Derek Brink

published by: RSA Press and McGraw-Hill

ISBN: 0072131233

Examination Details

Testing Centers, Locations, and Registration

The RSA Digital Certificate Management Solutions 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 Digital Certificate Management Solutions Certified Systems Engineer exam code is 050-V66-SERCMS01.

Exam Questions

The RSA Digital Certificate Management Solutions CSE exam consists of 76 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 Digital Certificate Management Solutions 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 accept the terms of an RSA Certified Security Professional Certification Non-Disclosure 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.