Vendor: RSA

Exam Code: 050-SEPROAUTH-02

Exam Name: RSA Certified SE Professional in Authentication Manager Solution

Version: Demo

1. CERTIFICATION REQUIREMENTS

(A)Obtaining Certification:

To obtain certification in any of the RSA Certified Security Professional designations, You must successfully comply with the initial certification requirements for that designation. Certification requirements are available on the RSA Certification Web site, or available from RSA, The Security Division of EMC at the address specified herein. By sending You the RSA Certified Security Professional Welcome Kit, RSA confirms that, according to its records, You have complied with the initial certification requirements for the RSA Certified Security Professional designation indicated in the RSA Certified Security Professional Welcome Kit.

(B)Maintaining Active Certification:

To maintain Your active certification(s), You must comply with any and all continuing certification requirements which shall be established by RSA, The Security Division of EMC and may include periodically taking a re-certification examination that tests Your knowledge of the features and functionality of any major product release. You acknowledge and agree that RSA may, in its sole discretion, change the certification requirements (both initial and continuing), RSA Certified Security Professional designations, and RSA Certified Security Professional Logos and Guidelines at any time. You are responsible for periodically checking the RSA Certified Security Professional website for updates and compliance with any and all updates. Failure to comply with all requirements will result in termination of this Agreement.

(C)Transfer of Certification:

You shall not transfer or share Your RSA Certified Security Professional certification and the benefits of such certification to or with another person or entity.

2.USE OF RSA CERTIFIED SECURITY PROFESSIONAL DESIGNATIONS and LOGOS

Upon Your successful completion of the initial certification requirements, and so long as You remain in compliance with all applicable continuing certification requirements, RSA, The Security Division of EMC hereby authorizes You to use the RSA Certified Security Professional designation for which You have obtained certification, as indicated in the RSA Certified Security Professional Welcome Kit which includes this RSA Certified Security Professional Agreement and the RSA Certified Security Professional Logo Guidelines which set forth the authorized use of the RSA Certified Security Professional Logo.

You acknowledge RSA's sole ownership of the RSA Certified Security Professional Logo and designations, and that nothing in the RSA Certified Security Professional Agreement, or in Your performance as an RSA Certified Security Professional, or that might otherwise be implied by law,

shall operate to give You any right, title or interest in the RSA Certified Security Professional designation(s) or Logo, other than the authorization specifically granted.

You shall use the RSA Certified Security Professional Logo and designation(s) in a manner that does not derogate from RSA's rights in the RSA Certified Security Professional Logo and designations, and shall take no action that may interfere with or diminish RSA's rights in the RSA Certified Security Professional Logo or designations, either during the term of the RSA Certified Security Professional Agreement or afterwards. You agree to immediately cease all use of the RSA Certified Security Professional designation(s) and Logo upon the expiration or termination of the RSA Certified Security Professional Agreement.

Nothing in the RSA Certified Security Professional Agreement authorizes You to use any RSA, The Security Division of EMC or EMC Corporation trademarks, service marks, or logos except as expressly Specified in the RSA Certified Security Professional Agreement and RSA Certified Security Professional Logo Guidelines.

3.LIMITATION OF LIABILITY

IN NO EVENT SHALL RSA, THE SECURITY DIVISION OF EMC BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO LOSS OF BUSINESS PROFITS) ARISING FROM OR RELATED TO YOUR CERTIFICATION, FAILURE TO ACHIEVE CERTIFICATION, OR USE OF OR INABILITY TO USE THE RSA CERTIFIED SECURITY PROFESSIONAL LOGO OR DESIGNATIONS, OR ARISING FROM OR RELATED TO THE TERMINATION OF YOUR CERTIFICATION, EVEN IF RSA, THE SECURITY DIVISION OF EMC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

4.INDEMNIFICATION

You agree to indemnify and hold RSA, The Security Division of EMC harmless against any loss, liability, damage, cost or expense (including reasonable legal fees) arising out of:

width

width

Your use of the RSA Certified Security Professional Logo and/or the RSA Certified Security

Professional designation(s) in a manner which is in any way inconsistent with the terms of the RSA Certified Security Professional Agreement;

width

width

By reason of Your performance or non-performance as a RSA Certified Security Professional; or

width

width

RSA Security's termination of the RSA Certified Security Professional Agreement.

In the event RSA, The Security Division of EMC seeks indemnification from You under this Section, RSA will immediately notify You in writing of any claim or proceeding brought against it for which it seeks indemnification. In no event may You enter into any third-party agreements that would, in any manner whatsoever, affect the rights of, or bind, RSA, The Security Division of EMC in any manner, without the prior written consent of RSA, The Security Division of EMC.

5. REPRESENTATIONS

All certified security professionals who are certified under the RSA Certified Security Professional Program recognize that such certification is a privilege that must be both earned and maintained. In support of this, You represent that all business You conduct in Your capacity as an RSA Certified Security Professional, and all services You provide concerning RSA's products, shall be performed in a manner that:

width

width

Does not, in any way, harm RSA's reputation;

width

width

Avoids deceptive, misleading, or unethical practices; width

width

Avoids making any representations, warranties, or guarantees to customers on behalf of RSA, The Security Division of EMC for RSA's products or otherwise;

width

width

Complies with all applicable U.S. export regulations and other applicable governmental laws and regulations; and

width

width

Complies with copyright and other intellectual property and proprietary rights protections for RSA's products.

6. NON-DISCLOSURE AGREEMENT

You expressly undertake to retain, in confidence, all information and know-how transmitted to You by RSA, The Security Division of EMC that RSA has identified as being proprietary and/or confidential or that, by the nature of the circumstances surrounding its disclosure, ought in good faith to be treated as proprietary and/or confidential, and You will make no use of such information and know-how except under the terms and during the existence of the Non-Disclosure Agreement.

You expressly acknowledge that the RSA Certified Security Professional certification test questions and materials are subject to these confidentiality and non-disclosure obligations, and may not be disclosed to or discussed with others, or posted or published in any forum or through any medium. Notwithstanding the foregoing, You shall have no obligation to maintain the confidentiality of information that:

width

width

Has become generally available to the public through no wrongful act on Your part;

width

width

Has been independently developed; or

width

width

Is known to be free of restrictions.

Further, You may disclose confidential information as required by governmental or judicial order, provided You give RSA prompt written notice prior to such disclosure, and comply with any protective order (or equivalent) imposed on such disclosure.

Your obligation under this Section shall survive the expiration or termination of the RSA Certified Security Professional Agreement and continue after any termination of said Agreement.

7. TERMINATION

Termination By Either Party:

width

Either party may terminate the RSA Certified Security Professional Agreement at any time, with or without cause.

Immediate Termination By RSA:

width

Without prejudice to any rights RSA, The Security Division of EMC may have under the RSA Certified Security Professional Agreement or in law, equity, or otherwise, and in addition to its rights outlined in the previous paragraph, RSA, The Security Division of EMC may terminate the RSA Certified Security Professional Agreement immediately, including termination of any certifications and RSA Certified Security Professional designations to which the Agreement relates, and termination of Your use of the corresponding RSA Certified Security Professional Logo, upon the occurrence of any one of the following events (the "Defaults"):

width

You fail to comply with the applicable continuing certification requirements for such certification; width

You otherwise fail to comply with any of the terms of the RSA Certified Security Professional Agreement, including, without limitation, the terms governing the use of the RSA Certified Security Professional designations and Logo;

width

You engage in misappropriation or unauthorized disclosure of any trade secret or confidential information of RSA (including, but not limited to, any RSA Certified Security Professional certification test materials or other RSA materials with respect to which You are under non-disclosure obligation), or pirate any RSA's product, or otherwise infringe any other intellectual property right of RSA, or engage in any other activities prohibited by law; or

width

A government agency or court finds that services You provided concerning RSA's products, to which Your certification relates, are defective in any way.

width

In the event any Default occurs, RSA, The Security Division of EMC will provide You with written notice of termination of the RSA Certified Security Professional Agreement.

Obligations Upon Termination

width

From and after termination of the RSA Certified Security Professional Agreement, You shall immediately cease all use of any RSA Certified Security Professional designation and Logo to which the Agreement relates.

8.GENERAL PROVISIONS

Governing Law:

width

The laws of the Commonwealth of Massachusetts will, in all respects, govern the RSA Certified Security Professional Agreement.

Compliance with Laws:

width

You agree that at all times You shall conduct Your business in compliance with all applicable federal, state and local laws and regulations, including, but not limited to, laws regulating Your professional status and designation.

width

You should note that some states and/or countries regulate the use of the term "engineer" and You should comply, as applicable, with any such laws in addition to the RSA Certified Security Professional Agreement and the RSA Certified Security Professional Logo Guidelines in connection with attaining the RSA Certified Systems Engineer designation(s).

Modifications:

width

Except as otherwise expressly provided in the RSA Certified Security Professional Agreement, the terms of said Agreement may be modified only by RSA's transmission to You setting out any modifications.

Modifications to the Agreement shall be effective 30 days following the date on which RSA, The Security Division of EMC transmits the modification notice.

width

If You do not wish to accept the modified Agreement, You shall send written notice of termination to RSA, The Security Division of EMC.9.

NOTICES

All notices required by the RSA Certified Security Professional Policies and Procedures and/or the RSA Certified Security Professional Agreement must be addressed to:

Dir. Educational Services Worldwide

RSA Certified Security Professional Program RSA, The Security Division of EMC

174 Middlesex Turnpike Bedford, MA 01730 USA

All notices will be sent to the e-mail or mailing address You provided at registration unless You have updated Your address by e-mailing RSA, The Security Division of EMC at: certification@rsa.com.

****

If You accept the above Terms and Conditions, please click the YES Button. By selecting YES, You agree to be bound by such Terms and Conditions stated above.

Click the NO button if you do not accept these terms.

****

A. Yes, I agree.

B. No, I do not agree.

Note: You must accept the terms of the RSA Certified Security Professional Agreement - as stated above

- to continue with this exam.

Answer: A

2. In RSA Authentication Manager, On-Demand Authentication can be (Choose two)

A. a primary authentication method for web access.

B. a substitute for an RSA SecurID hardware token PIN.

C. a step-up authentication method for Risk-Based Authentication. D.sent simultaneously to a user's e-mail account and mobile phone.

E. used in place of Security Question enrollment in the Self-Service console.

Answer: AC

3. RSA SecurID two-factor authentication requires

A. two valid user-defined passwords.

B. an RSA SecurID PASSCODE and PIN.

C. an RSA SecurID token's tokencode and PIN.

D. a Realm Administrator account and an Authentication Agent

Answer: C

4. To process a user authentication, an RSA SecurID hardware token requires

A. a CT-KIP implementation.

B. a link to an Active Directory account.

C. an RSA Authentication Manager server.

D. a valid mobile phone number for the user.

Answer: C

5. An "Assurance Level" is associated with which aspect of RSA technology?

A. Risk-Based authentication

B. Trusted Realm relationship

C. RSA Certified Partner products

D. Authentication Agent communication

Answer: A

6. An organization with a large user population that requires multiple Replica servers, On-Demand Authentication (ODA), and protection using Risk-Based Authentication (RBA) would be best served by which of the following solutions?

A. RSA Authentication Manager with a Base license and ODA plug-in

B. RSA Authentication Manager with an Enterprise license and Replica package

C. RSA Authentication Manager with an Enterprise license and ODA/RBA option

D. RSA Authentication Manager with a Web Tier deployment, Base license and RBA plug-in

Answer: C

7. When using an RSA Authentication Agent for PAM, which of the following statements is true?

A. The Agent for PAM supports Microsoft EAP and Remote Access protocols.

B. Users designated for RSA SecurID authentication must have root privileges.

C. A user's account is limited to RSA SecurID authentication through Web Access.

D. Users accessing a local workstation can be challenged for RSA SecurID authentication.

Answer: D

8. If a user is issued an RSA SecurID SID800 Hybrid token, the user must log in using a computer with a USB 2.0 port and the SID800 token must be plugged in to that port to allow use of the one time passcode.

A. True
B. False

Answer: B

9. Which of the following is NOT a component of the technology used within an RSA SecurID token?

A. algorithm
B. private key
C. time source
D. seed record

Answer: B

10. Token expiration dates

A. vary according to the date contained in the license.rec file.
B. are established when the new user first uses the token to log on.
C. are re-set by the Administrator using the 'Resynchronize Token' function.
D. are programmed into a token's seed record at the time the record is created.

Answer: D

11. RSA Authentication Manager time synchronous tokencode calculations

A. require a token "Seed" value as well as a time component.
B. always uses the NTP (Network Time Protocol) to provide the time component.
C. depend on an accurate time setting of the RSA Authentication Agent host computer.

D. can only be made by RSA SecurID Software Tokens with access to a host computer clock.

Answer: A

12. The RSA Authentication Agent for Microsoft Windows DOES NOT protect which of the following types of authentication?

A. Authentication on a Microsoft Windows workstation
B. Access to Microsoft Internet Information Server (IIS)
C. Connection to Microsoft Remote Authentication Server (RAS)
D. Authentication using Microsoft Extensible Authentication Protocol (EAP)

Answer: B

13. The RSA Authentication Manager Self-Service function allows

A. users to request RSA SecurID tokens.
B. managers to control the deployment of Replica servers.
C. administrators to install software token packages remotely.
D. Agents to determine what credentials are valid for authentication.

Answer: A

14. The RSA Authentication Agent for Web is intended to

A. prevent designated web content from being downloaded to an end user's computer.
B. challenge a user for authentication if the user attempts to access specific web content.
C. challenge a user for authentication if the user attempts to log on locally to the web server host computer.
D. allow users to access low risk resources using a password and high risk resources using two factor authentication.

Answer: B

15. The Offline Authentication feature is intended to allow

A. the capability for a user to temporarily disable the Agent software while the user is working offline.
B. an RSA SecurID authentication to be processed by a Replica server when the Primary server is off line.
C. a user to complete an RSA SecurID authentication through the local Agent if the local Agent computer is offline.
D. several users to use a single RSA SecurID token so that they can share another user's computer if their own computer is off line.

Answer: C

16. In an RSA Authentication Manager environment, data replication to provide failover capability can take place between

A. Security Domains
B. Offline data stores
C. Authentication Agents
D. Primary and Replica instances

Answer: D

17. If an RSA Authentication Manager deployment plan indicates that an organization is best served by installing a Primary instance and three Replica instances, which of the following statements is true?

A. A Base license will allow installation of these four instances.
B. An Enterprise license is required to install these four instances.
C. An additional Base license is required to install each additional Replica instance.
D. A Business Continuity Option (BCO) license is required to install a Replica instance.

Answer: B

18. The CT-KIP protocol is most closely associated with?

A. RSA SecurID software tokens.
B. RADIUS client communication.
C. On-Demand user authentication.
D. RSA Authentication Manager Quick Setup.

Answer: A

19. In what way is the RSA Authentication Manager "Internal Database" different from an external Identity Source?

A. The Internal Database contains policy and token data in addition to user and group data.
B. The Internal Database can contain Identity Attributes while the external Identity Source can not.
C. The external Identity Source is a read/write datastore while the Internal Database is always read-only.
D. The Internal Database utilizes LDAP while the external Identity Source can be configured for either LDAP or RDMBS.

Answer: A

20.A Web Tier Load Balancer

A. distributes authentication requests among any available web servers.
B. distributes connections between Primary and Replica web tier servers.
C. is required whenever deploying RSA Authentication Manager Express in a DMZ.
D. responds to authentication attempts if Primary and Replica instances are off line or unavailable.

Answer: B

21. Reports in RSA Authentication Manager are customized

A. through creating Regular Expression filters.

B. by modifying report templates in the administrative console.

C. by editing the Events database files and digitally re-signing them.

D. through use of the Report Manager utility in the Operations Console.

Answer: B

22. In RSA Authentication Manager, the Self-Service function allows

A. user self-service only if the deployment has an Enterprise license.

B. business continuity options only if the deployment has a Base license.

C. authenticator provisioning only if the deployment has an Enterprise license.

D. authenticator provisioning and distribution only if the deployment has a Business Continuity Option.

Answer:C

23. The value of an on-demand tokencode is

A. its ability to be re-used for login up to 5 times before expiration.

B. that multiple users can share the same tokencode in an emergency.

C. that it can be supplied to users who have no assigned authenticator.

D. the added security of a hardware token that only displays a tokencode when activated.

Answer:C

24.A "Device Fingerprint" is most closely associated with which of the following?

A. RSA Risk-Based Authentication

B. RSA Authentication Agent auto-registration

C. an On-Demand code sent to a mobile device

D. a device on which an RSA SecurID token is installed

Answer:A

25. The term "Silent Collection" relates to

A. Risk-Based behavioral data.
B. Authentication Agent actions.
C. Administrator activity audit logs.
D. Primary-to-Replica database reconciliation.

Answer:A

26. If an organization wants to use RSA SecurID tokens without a PIN (tokencode only),

A. RSA Authentication Manager will not allow it.
B. their token choice is limited to only software tokens.
C. they should be advised that it is not a best security practice.
D. the user can leave their PIN setting blank when prompted to set a PIN.

Answer: C

27. The Adjudicator service is a process designed to

A. lock the RSA SecurID token if it is suspected stolen.
B. securely store and update the database encryption key.
C. prevent the same passcode from being replayed on different servers.
D. resolve database differences between an Authentication Manager server and Server Node.

Answer: C

28. VMware ESXi is used as part of an RSA Authentication Manager deployment because

A. ESXi provides the required firewall protection.
B. the Web Tier server can only be installed on ESXi.
C. Authentication Manager is distributed as a virtual appliance.
D. VMware provides a faster response time to Authentication Agents.

Answer: C

29. The policy to define a user's PIN parameters (for example, length and composition) is managed

A. as a System Setting.
B. as part of the Token Policy.
C. as a part of Security Domain Policy.
D. as part of the User Authentication Policy.

Answer: B

30. One advantage of creating and running a report compared to a simple console search is that

A. console searches do not allow data filtering.
B. reports can return more results than a console search.
C. report generation is always faster than a console search.
D. console searches can only display results in real time – not historical data.

Answer: B

31. For which of the following situations is creating a 'package' file necessary before installation or deployment can begin? (Choose two)

A. RADIUS client installation
B. Replica instance deployment
C. Primary server deployment

D. Authentication Agent installation

E. Authentication Manager Web Tier installation

Answer: BE

32. The RSA Self-Service console most closely relates to

A. Authentication activity between an Agent and server.

B. Provisioning activity between a user and an authentication method.

C. Data connections between Active Directory and authentication credentials.

D. Deployment workflow for authentication servers and Web Tier load balancing.

Answer: B

33. In a Primary/Replica environment, administrative changes can be made only on a Primary server.

A. True

B. False

Answer: A

34. Designating an "Alternate IP Address" value in an Agent record in the Authentication Manager Security Console allows

A. an Authentication Agent to use multiple node secret files.

B. an Authentication Agent to seek the fastest responding server.

C. an Authentication Agent to communicate with multiple servers simultaneously.

D. Authentication Manager to recognize translated or multi-homed IP addresses for Agent authentication requests.

Answer: D

To Read the **Whole Q&As**, please purchase the **Complete Version** from **Our website**.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

Guarantee & Policy | Privacy & Policy | Terms & Conditions