Exam Code: SC0-501

Exam Name: Enterprise SecurityImplementation

Vendor: SCP

Version: DEMO

Part: A

1: Using your digital certificate, when you wish to prove your identity with a digital signature, which of the following are true?

A.You create a hash value of your message and encrypt the hash with your private key

B.Anyone who has your private key can decrypt the hash

C.You create a hash value of your message and encrypt the hash with your public key

D.Anyone who has your public key can decrypt the hash

E.The recipient can make a new hash and match it to the hash you sent, verifying the message is unaltered and came from you.

Correct Answers: A D E

2: If a user leaves your organization, and you wish to reuse the token that was returned, what will your first step be?

A.Delete the token

B.Disable the token

C.Destroy the token

D.Reinitialize the token

E.Unassign the token

Correct Answers: E

3: Where in a digital certificate will you find values such as md5WithRSAEncryption or sha1WithRSAEncryption?

A.In the Issuer field

B.In the Signature field

C.In the Subject field

D.In the Validity field

E.In the SubjectPublicKeyInfo field

Correct Answers: B

4: When a biometric system performs a one-to-one mapping, what is the systems doing?

A.Identification

B.Authentication

C.Classification

D.Detection

E.Recognition

Correct Answers: B

5: You are building a trusted network in your organization. Which of the following technologies are required to build the trusted network?

A.Intrusion Detection

B.Cryptography

C.Strong Authentication

D.Digital Certificates

E.Virtual Private Networks

Correct Answers: B C D

6: If you are using a smart card that does not make a physical connection to a reader, what type of card are you using?

A.Prism-based card

B.Hermes-based card

C.Non-volatile card

D.Contactless card

E.Optical card

Correct Answers: D

7: If you have just installed your SecureID system, and are ready to use the token for the very first time, you will be prompted for which of the following?

A.New PIN mode

B.New Tokencode

C.New Passcode

D.To reboot the server

E.To reboot the client

Correct Answers: A

8: Functions typically supported by a smart card reader include which of the following?

A.Powers the smart card.

B.Provides communication.

C.Provides a system clock.

D.Supports biometrics.

E.Supports forensics data sampling.

Correct Answers: A B C E

9: What are the two methods that can be used to deliver a CRL?

A.Direct

B.Pushing

C.Immediate Revocation List

D.Indirect

E.Polling

F.Scheduled Revocation List

Correct Answers: B E

10: What from the following list is not a core function of the Incident Response Team?

A.Staying current on Attack Techniques

B.Creation of the Security Policy

C.Education of Employees

D.Implement Security Controls

E.Communicate with the Organization

Correct Answers: D

11: Which of the following are symmetric encryption algorithms?
A.MD5
B.RSA
C.Diffie-Hellman
D.3DES
E.AES
Correct Answers: D E

12: There are three logical sections to an X.509v3 digital certificate, the certificate itself, the variable options, and the fixed fields. Which of the following are found in the fixed fields?
A.The SubjectPrivateKeyInfo
B.The SignatureAlgorithm
C.The SerialNumber
D.The SubjectPublicKeyInfo
E.The SignatureValue
Correct Answers: C D

13: What is the default algorithm used to sign PGP messages?
A.MD5
B.RSA
C.SHA1
D.DH
E.IDEA
Correct Answers: C

14: What are the four methods of Public Key Distribution?
A.Public Announcement
B.Public Key Storage
C.Public Key Directory
D.Public Key Authority
E.Public Key Certificates
Correct Answers: A C D E

15: What do wireless access points use to counter multipath interference?
A.Multiple encryption algorithms
B.Multiple Antennas
C.Multiple radio frequencies
D.Duplicate packet transfer
E.Secondary transmissions
Correct Answers: B