\_\_\_\_\_\_\_\_\_\_ is a process where authentication and permission will be passed on from one system to another, usually across multiple enterprises, thereby reducing the number of authentications needed by the user.

Incorrect answer:

SSO

Correct Answer:Federation

**Results for question 2.**

2

1 / 1 point

An \_\_\_\_\_\_\_\_\_\_ manages the creation and maintenance of attributes such as passwords and biometric information.



authorizing agent

, Not Selected

Correct answer:



attribute service



identity provider

, Not Selected



authenticator

, Not Selected

**Results for question 3.**

3

1 / 1 point

Used in most network security applications, the \_\_\_\_\_\_\_\_\_\_ standard has become universally accepted for formatting public-key certificates.



X.905

, Not Selected



PKIX

, Not Selected



IETF

, Not Selected

Correct answer:



X.509

**Results for question 4.**

4

1 / 1 point

The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of users to access a number of servers and for the servers to exchange data with each other.

Correct answer:

True

False

**Results for question 5.**

5

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ knows the passwords of all users and stores these in a centralized database and also shares a unique secret key with each server.



ticket server

, Not Selected



management server

, Not Selected

Correct answer:



authentication server



key distribution server

, Not Selected

**Results for question 6.**

6

0 / 1 point

A \_\_\_\_\_\_\_\_\_ consists of a public key plus a user ID of the key owner, with the whole block signed by a trusted third party which is typically a CA that is trusted by the user community.

Incorrect answer:

Public-key certificate

Correct Answer:public-key certificate, certificate

**Results for question 7.**

7

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals, with a focus of defining an identity for each user, associating attributes with the identity, and enforcing a means by which a user can verify identity.



PKIX management

, Not Selected



Registration authority

, Not Selected

Correct answer:



Identity management



Federated managing authority

, Not Selected

**Results for question 8.**

8

1 / 1 point

If an opponent captures an unexpired service granting ticket and tries to use it, they will be denied access to the corresponding service.

True

Correct answer:

False

**Results for question 9.**

9

1 / 1 point

The \_\_\_\_\_\_\_\_\_ extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.



policy mappings

, Not Selected

Correct answer:



certificate policies



directory attribute

, Not Selected



authority key identifier

, Not Selected

**Results for question 10.**

10

1 / 1 point

If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True

Correct answer:

False

The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of users to access a number of servers and for the servers to exchange data with each other.

Correct answer:

True

False

### Results for question 2.

2

0 / 1 point

When two end systems wish to communicate they establish a logical connection and, for the duration of that logical connection, all user data are encrypted with a one-time \_\_\_\_\_\_\_\_\_\_ which is destroyed at the end of the session.

Incorrect answer:

session keys

Correct Answer:session key

### Results for question 3.

3

1 / 1 point

User certificates generated by a CA need special efforts made by the directory to protect them from being forged.

True

Correct answer:

False

### Results for question 4.

4

0 / 1 point

\_\_\_\_\_\_\_\_\_\_ is a process where authentication and permission will be passed on from one system to another, usually across multiple enterprises, thereby reducing the number of authentications needed by the user.

Incorrect answer:

Federation / SSO

Correct Answer:Federation

### Results for question 5.

5

1 / 1 point

Once the authentication server accepts the user as authentic, it creates an encrypted \_\_\_\_\_\_\_\_\_ which is sent back to the client.



access code

, Not Selected

Correct answer:



ticket



password

, Not Selected



key

, Not Selected

### Results for question 6.

6

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is the client's choice for an encryption key to be used to protect this specific application session.

Correct answer:

subkey

### Results for question 7.

7

1 / 1 point

The principal underlying standard for federated identity is the Security Assertion Markup Language (SAML) which defines the exchange of security information between online business partners.

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

The \_\_\_\_\_\_\_\_\_ extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.



policy mappings

, Not Selected



authority key identifier

, Not Selected

Correct answer:



certificate policies



directory attribute

, Not Selected

### Results for question 9.

9

1 / 1 point

\_\_\_\_\_\_\_\_\_\_ defines a framework for the provision of authentication services by the X.500 directory to its users and defines alternative authentication protocols based on the use of public-key certificates.

Correct answer:

X.509

### Results for question 10.

10

1 / 1 point

Containing the hash code of the other fields encrypted with the CA's private key, the \_\_\_\_\_\_\_\_\_\_ covers all of the other fields of the certificate and includes the signature algorithm identifier.

Correct answer:



signature



extension

, Not Selected



subject unique identifier

, Not Selected



issuer unique identifier

An \_\_\_\_\_\_\_\_\_\_ manages the creation and maintenance of attributes such as passwords and biometric information.



identity provider

, Not Selected



authorizing agent

, Not Selected



authenticator

, Not Selected

Correct answer:



attribute service

### Results for question 2.

2

0 / 1 point

With a principal objective of enabling secure, convenient, and efficient acquisition of public keys, \_\_\_\_\_\_\_\_\_\_ is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

Incorrect answer:

Public key infrastructure

Correct Answer:public-key infrastructure, PKI

### Results for question 3.

3

1 / 1 point

If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True

Correct answer:

False

### Results for question 4.

4

1 / 1 point

After determining which systems are allowed to communicate with each other and granting permission for the two systems to establish a connection, the \_\_\_\_\_\_\_\_\_ provides a one-time session key for that connection.

Correct answer:

KDC

### Results for question 5.

5

1 / 1 point

Kerberos version 4 requires the use of a(n) \_\_\_\_\_\_\_\_\_\_\_\_.



MAC address

, Not Selected

Correct answer:



IP address



ISO network address

, Not Selected



Ethernet link address

, Not Selected

### Results for question 6.

6

0 / 1 point

The strength of any cryptographic system rests with the \_\_\_\_\_\_\_\_\_ technique, a term that refers to the means of delivering a key to two parties that wish to exchange data without allowing others to see the key.

Incorrect answer:

Key distribution

Correct Answer:key distribution

### Results for question 7.

7

1 / 1 point

If an opponent captures an unexpired service granting ticket and tries to use it, they will be denied access to the corresponding service.

True

Correct answer:

False

### Results for question 8.

8

0 / 1 point

The \_\_\_\_\_\_\_\_\_ extension is used only in certificates for CAs issued by other CAs and allows an issuing CA to indicate that one or more of that issuer's policies can be considered equivalent to another policy used in the subject CA's domain.

Incorrect answer:

Policy mapping

Correct Answer:policy mappings

### Results for question 9.

9

1 / 1 point

A \_\_\_\_\_\_\_\_\_ is the client's choice for an encryption key to be used to protect this specific application session.

Correct answer:

subkey

### Results for question 10.

10

1 / 1 point

The technical deficiencies of Kerberos version 4 are: double encryption, PCBC encryption, session keys, and \_\_\_\_\_\_\_\_\_\_.

Correct answer:

password attacks