**Chapter 23 – Internet Authentication Applications**

**TRUE/FALSE QUESTIONS:**

T F 1. The approach taken by Kerberos is using authentication software tied

to a secure authentication server.

T F 2. The overall scheme of Kerberos is that of a trusted third-party

authentication service.

T F 3. Kerberos is designed to counter only one specific threat to the security

of a client/server dialogue.

T F 4. An obvious security risk is that of impersonation.

T F 5. The authentication server shares a unique secret key with each server.

T F 6. The ticket-granting ticket is encrypted with a secret key known only to

the AS and the TGS.

T F 7. The ticket-granting ticket is not reusable.

T F 8. Kerberos does not support interrealm authentication.

T F 9. X.509 provides a format for use in revoking a key before it expires.

T F 10. Because serial numbers are unique within a CA, the serial number is

sufficient to identify the certificate.

T F 11. The principal objective for developing a PKI is to enable secure,

convenient, and efficient acquisition of private keys.

T F 12. Initialization begins the process of enrolling in a PKI.

T F 13. Update is not required when the certificate lifetime expires or as a

result of certificate revocation.

T F 14. CMP, defined in RFC 2510, is designed to be a flexible protocol able

to accommodate a variety of technical, operational, and business models.

T F 15. Federated identity management makes use of a number of standards

that provide the building blocks for secure identity information exchange across different domains or heterogeneous systems.

**MULTIPLE CHOICE QUESTIONS:**

1. One of the earliest and most widely used services is \_\_\_\_\_\_\_\_\_.

A. Kerberos B. FIM

C. PKI D. X.509

1. \_\_\_\_\_\_\_ is important as part of the directory service that it supports and is also a basic building block used in other standards.

A. PKI B. X.509

C. Kerberos D. FIM

3. \_\_\_\_\_\_\_\_ requires that a user prove his or her identity for each service invoked and, optionally, requires servers to prove their identity to clients.

A. FIM B. Kerberos

C. X.509 D. PKI

4. Kerberos uses the \_\_\_\_\_\_\_ encryption algorithm.

A. AES B. PKI

C. DES D. TGS

5. \_\_\_\_\_\_\_ certificates are used in most network security applications, including IP security, secure sockets layer, secure electronic transactions, and S/MIME.

A. X.509 B. PKI

C. FIM D. SCA

6. The \_\_\_\_\_\_\_ consists of two dates: the first and last on which the certificate is valid.

A. version B. period of validity

C. extension D. unique identifier

7. An integer value unique within the issuing CA that is unambiguously associated with the certificate is the \_\_\_\_\_\_\_\_.

A. issuer name B. subject’s public-key information

C. issuer unique identifier D. serial number

8. A \_\_\_\_\_\_\_ is a generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

A. RA B. registration

C. repository D. CA

9. \_\_\_\_\_\_\_ is the process in which a CA issues a certificate for a user’s public key and returns that certificate to the user’s client system and/or posts that certificate in a repository.

A. Certification B. Registration

C. Initialization D. Authorization

10. \_\_\_\_\_\_\_ is the process whereby a user first makes itself known to a CA prior to that CA issuing a certificate or certificates for that user.

A. Authorization B. Registration

C. Certification D. Initialization

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

A. Integration B. Registration

C. Synchronization D. Federation

12. \_\_\_\_\_\_\_ is a minimal set of conventions for invoking code using XML over HTTP that enables applications to request services from one another with XML-based requests and receive responses as data formatted with XML.

A. SOAP B. SAML

C. HTML D. WS-Security

13. \_\_\_\_\_ is a markup language that uses sets of embedded tags or labels to characterize text elements within a document so as to indicate their appearance, function, meaning, or context.

A. HML B. HTTP

C. XML D. SOAP

14. A principal element of an identity management system is \_\_\_\_\_\_\_.

A. workflow automation B. delegated administration

C. authentication D. all of the above

15. \_\_\_\_\_\_\_ is movement of data in a business process.

A. Provisioning B. Workflow automation

C. Revocation D. Initialization

**SHORT ANSWER QUESTIONS:**

1. \_\_\_\_\_\_\_ systems are automated methods of verifying or recognizing identity on the basis of some physiological or behavioral characteristic.
2. A software utility initially developed at MIT and available both in the public domain and in commercially supported versions, \_\_\_\_\_\_\_\_ is the defacto standard for remote authentication.
3. An alternative to each server being required to confirm identities of clients who request service is to use an \_\_\_\_\_\_\_ that knows the passwords of all users and stores them in a centralized database.
4. A full-service Kerberos environment consisting of a Kerberos server that has the user ID and password of all participating users in its database and shares a secret key with each server, all users and servers being registered with the Kerberos server, is referred to as a Kerberos \_\_\_\_\_\_.
5. The \_\_\_\_\_\_\_\_\_ is an optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
6. \_\_\_\_\_\_ is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.
7. The certification \_\_\_\_\_\_\_\_\_ is the issuer of certificates and certificate revocation lists.
8. \_\_\_\_\_\_\_\_ allows end entities to restore their encryption/decryption key pair from an authorized key backup facility.
9. The focus of \_\_\_\_\_\_\_\_\_ is defining an identity for each user, associating attributes with the identity, and enforcing a means by which a user can verify identity.
10. In a generic identity management architecture a \_\_\_\_\_\_\_\_ is an identity holder.
11. In a generic identity management architecture \_\_\_\_\_\_\_ are entities that obtain and employ data maintained and provided by identity and attribute providers, often to support authorization decisions and to collect audit information.
12. \_\_\_\_\_\_\_ is an XML-based language for the exchange of security information between online business partners.
13. \_\_\_\_\_\_\_\_ is a set of SOAP extensions for implementing message integrity and confidentiality in Web services.
14. In Kerberos, the \_\_\_\_\_\_\_\_\_\_\_ decrypts the ticket and authenticator, verifies the request, and creates ticket for requested server.
15. The ticket contains the user’s ID, the server’s ID, a \_\_\_\_\_\_\_\_\_\_, a lifetime after which the ticket is invalid, and a copy of the same session key sent in the outer message to the client.