**JECRC University, Jaipur**

**School of Computer Applications**

**MCA – III Semester**

**Unit – IV Assignment (Public Key Infrastructure)**

**Subject: Internet Security and Cryptography**

**Date of Release: 03 Dec. 22 Last Date of Submission 7th Dec 2022**

**Section – A**

1. [CO4] Digital certificates solve the problem of key exchange.
   1. Key Exchange
   2. Key Generation
   3. Key Recovery
   4. Key Recording
2. [CO4]The latest version of X.509 standard is –
   1. Version 1
   2. Version 2
   3. Version 3
   4. Version 4
3. [CO4] A CA has to provide services of –
   1. key management
   2. archival
   3. storage and retrieval
   4. All of above
4. [CO4] A digital certificate associate –
   1. a user's public key with his private key
   2. the user's identity with his public key
   3. a user's private key with the public key
   4. a private key with a digital signature
5. [CO4] X.509 protocol is used to specify –
   1. The structure of digital certificates
   2. The encryption algorithm
   3. Message Digest
   4. All of above
6. [CO4] The CA signs a digital certificate with –
   1. the user’s public key
   2. the user’s private key
   3. its own private key
   4. its own public key
7. [CO4] Requesting for a certificate result into the creation of a file.
8. PKCS#7
9. PKCS#9
10. PKCS#10
11. PKCS#12
12. [CO4] The of the user should never appear in a certificate.
    1. public key
    2. private key
    3. organization name
    4. name
13. [CO4] We trust a digital certificate because it contains –
    1. owner’s public key
    2. CA’s public key
    3. CA’s signature
    4. owner’s signature
14. [CO4] OCSP is –
    1. online
    2. online and offline
    3. offline
    4. not defined
15. [CO4] Which of these systems use timestamps as an expiration date?
    1. Public-Key-Certificates
    2. Public-announcements
    3. Publicly-available-directories
    4. Public-Key authority
16. [CO4] Which of them is not a major way of stealing email information?
    1. Stealing cookies
    2. Reverse Engineering
    3. Password Phishing
    4. Social Engineering
17. [CO4] Which of them is not a proper method for email security?
    1. Use Strong password
    2. Use email Encryption
    3. Spam filters and malware scanners
    4. Click on unknown links to explore
18. [CO4] WAP is a \_\_\_ type of protocol?
    * 1. Circuit switching
      2. Packet Switching
      3. Message switching
      4. Both a and b
19. [CO4] Which of the following is not a strong security protocol? a) HTTPS
    * 1. SSL
      2. SMTP
      3. SFTP

**Section – B**

1. [CO4] Define the format of Digital Certificate.

Graphical user interface

Description automatically generated with medium confidence

Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key the certificate issuer created.

1. [CO4] How RA reduce the work load of CA?

RA **verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it**.

1. [CO4] Discuss the steps used in creation of digital certificate.

**you send a document for signature in three easy steps:**

1. **Upload your document** into the electronic signature application
2. **Drag in the signature**, text and date fields where the recipient needs to take action.
3. **Click send**. The electronic signature application will email a link to the recipient so they can access the document and sign.
4. [CO4] Discuss any one mechanism used by a RA for checking the user’s proof of possession of the private key.

RA can use OpenSSL to show proof-of-possession (POP) of a private key by **signing a test file with it**. This method works for both RSA and ECC keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

1. [CO4] What is the idea behind Certification Authority hierarchy? .

A CA hierarchy **enables you to have a level of segmentation between different uses cases for the PKI**. This applies both to administration and the role of certificate authority. Separating administration roles allows different people or functions to manage a certificate authority.

**Section – C**

1. [CO4] A digital certificate should be self-signed. Explain the cause.

A self-signed SSL certificate is a digital certificate that’s not signed by a publicly trusted Certificate Authority (CA). Self-signed certificates are considered different from traditional CA signed certificates because they are created, issued, and signed by the company or developer who is responsible for the website or software associated with the certificate, rather than a CA.  they are available at no cost and can be requested easily by any developer. They are able to be implemented on your own timetable.

Self-signed certificates do not expire or need to be renewed after a set period of time, as is required by a CA certificate. Although this seems convenient, it is one of the major concerns with this option, as they cannot comply with security updates in response to discovered vulnerabilities, nor meet the [certificate agility](https://www.forbes.com/sites/forbestechcouncil/2021/07/09/certificate-agility-is-just-as-important-as-crypto-agility/?sh=6f89a6826257) needed to secure today's modern enterprise. As such, this method of authentication is rarely recommended.

1. [CO4] Describe how cross-certification is useful.

**A certificate issued from a certificate authority (CA) that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs**. Cross-certificates **provide a means to create a chain of trust from a single, trusted, root CA to multiple other CAs**.

1. [CO4] What are the common causes for revoking a digital certificate?

The validity period ends

The issuing CA has been compromised

The certificate owner no longer owns the [domain](https://www.techtarget.com/whatis/definition/domain) for which it was issued

The certificate owner has ceased operations entirely

The original certificate has been replaced with a new certificate from another issuer

1. [CO4] What are the broad level differences between CRL, OCSP and SCVP?

|  |  |
| --- | --- |
| OCSP can be used to get the status of a single certificate. | A CRL is a list with multiple lines that has to be downloaded by the browser. |
| Status of a certificate is fetched by making a request to an OCSP Responder. | A CRL is distributed using a CDP point which can be an HTTP link or an LDAP server. |
| Has less effect on the client and network resources. | Has a big effect on client resources. |
| Is the industry standard for Certificate Lifecycle Management currently. | Used to be the only solution for Certificate Lifecycle Management. |

1. [CO4] List out the public key cryptography standers (PKIS) and their purpose.

| **PKCS**#**1: RSA Cryptography Standard.**This standard defines mechanisms to encrypt and sign data using the RSA public key system. |
| --- |
| **PKCS #2 and #4: Incorporated into PKCS #1 (no longer exist).**These standards covered RSA encryption of message digests. They were merged into PKCS #1 and are no longer active. |
| **PKCS**#**3: Diffie-Hellman Key Agreement Standard.** The standard defines the [Diffie-Hellman key agreement protocol](https://www.techtarget.com/searchsecurity/definition/Diffie-Hellman-key-exchange) that enables two parties to agree on a secret key known only to them. PKCS #3 was superseded by modern key establishment schemes specified in IEEE 1363a, ANSI X9.42, ANSI X9.44, ANSI X9.63, etc. |
| **PKCS**#**5: Password-based Cryptography Standard.**This standard applies [pseudo random](https://www.techtarget.com/whatis/definition/pseudo-random-number-generator-PRNG) functions -- hash-based message authentication code, [cipher](https://www.techtarget.com/searchsecurity/definition/cipher) or [hash](https://searchsqlserver.techtarget.com/definition/hashing) -- to the input password, along with a salt value, to produce a derived key that can be used as a cryptographic key. The standard involves additional computation that makes password cracking more difficult, thus providing more enhanced security for password-based cryptographic primitives. |
| **PKCS**#**6: Extended-Certificate Syntax Standard.** Since the introduction of [X.509](https://www.techtarget.com/searchsecurity/definition/X509-certificate) v3, PKCS #6 is being phased out. |
| **PKCS**#**7: Cryptographic Message Syntax Standard.** This standard defines a generic syntax for cryptographic messages. It is superseded by Request for Comments 3369 for Cryptographic Message Syntax. |
| **PKCS**#**8: Private-Key Information Syntax Standard.** PKCS #8 defines a method to store private key information, including a private key for some public key algorithms. It also includes the syntax for encrypted private key information. |
| **PKCS**#**10: Certification Request Syntax Standard.** PKCS #10 defines the syntax for certification requests. When an entity needs a public key certificate, it constructs a certification request and sends it to the certification authority ([CA](https://www.techtarget.com/searchsecurity/definition/certificate-authority)), which transforms the request into an X.509 public key certificate. The standard does not specify the form in which the CA returns the new certificate. |

**Section – D**

1. [CO4] Consider a situation: an attacker ***A*** creates a certificate, puts a genuine organizations name, say ***bank B*** and the puts the attacker’s own public key. You get this certificate from the attacker, without knowing that the attacker is sending it. You think it is from the ***bank B***. How can this be prevented or resolved?
2. [CO4] In the other situation, the attacker ***A*** changes the bank’s genuine certificate ***B*** by replacing the bank’s public key in the certificate with his own. How can this be prevented or resolved?