What is public-key infrastructure?

Step 1:

Digital certificates are issued by public key infrastructure (PKI) regulations to safeguard sensitive information, offer distinct digital identities for users, devices, and apps, and ensure secure end-to-end communications.

Step 2:

Digital certificates that confirm the identification of users, devices, or services can be issued using PKI. These certificates can be used for both private internal services and public web pages (e.g., to authenticate devices connecting with your VPN, Wiki, Wi-Fi, etc.)

Secure Shell is used by PKI, or public key infrastructure, to authenticate logins and grant users the appropriate privileges. Data and information can now be transferred across cloud-based services and the Internet of Things with more safety thanks to this increased protection.

List the different management functions of the PKIX model.

Step 1:

Public Key Infrastructure X.509 is known as PKIX. The X.509 standard specifies the fields, structure, and distribution methods for public keys in addition to the structure, format, and fields for digital certificates. The PKIX working group is established by the IETF (Internet Engineering Task Force) in order to expand these standards and make them universal.

Step 2:

PKIX lists a number of management tasks that can require support from management protocols.

Registration:

This is the procedure by which a user initially identifies themselves to a CA (directly or through a RA), before that CA issues a certificate or certificate for that user. A PKI enrolment procedure begins with registration. Typically, some offline or online mechanism for mutual authentication is required for registration. The end entity often receives one or more shared secret keys that are utilized for later authentication.

Initialization:

In order for a client system to operate safely, key materials that are compatible with other infrastructure keys must be installed first. For application in validating certificate paths, the client, for instance, must be securely initialized with the public key and other assured information of the trusted CA(s).

Certification:

This is the technique a CA employs to generate a certificate for a user's public key, deliver that certificate back to the user's client machine, and/or submit it to a repository.

key pair recovery

Key pairs can be used for both encryption and decryption as well as the production and verification of digital signatures. If there is no way to retrieve the necessary decryption keys when regular access to the keying material is lost when a key pair is used for encryption and decryption, it will be impossible to recover the encrypted data.

Forgotten passwords or PINs, damaged hardware tokens, corrupted disc drives, and other issues can make it impossible to access the decryption key. Key pair recovery enables end entities to retrieve their encryption/decryption key pair from a trusted key backup repository (usually the CA that issued the end entity's certificate).

Key pair update:

: New key pairs must be issued and all existing key pairs must be updated on a regular basis. Updates are necessary when a certificate's lifetime expires and after a certificate is revoked.

Revocation request:

A CA is informed of an anomalous condition requiring the revocation of a certificate by a designated person. Private-key compromise, a change in association, and a name change are all grounds for revocation.

Cross certification:

It is the process through which two CAs share data to create a cross-certificate. A cross-certificate is a document that contains a CA signature key used to issue certificates and is issued by one CA to another CA.

Name the PKIX certificate management protocols.

Step 1:

Two other management protocols between PKIX entities that support the management functions specified in the preceding subsection have been defined by the PKIX working group. The certificate management protocols are described in RFC 2510. (CMP). Each management function in CMP is specifically identified by a different protocol exchange. The goal of CMP is to create a versatile protocol that can support a range of technological, operational, and financial models.

Step 2:

Certificate management messages over CMS (CMC) are defined in RFC 2797, where CMS is the cryptographic message syntax defined in RFC 2630. The foundation of CMC is older work, and it makes use of current implementations. All PKIX functions are supported, however not all of them correspond to particular protocol exchanges.

What is federated identity management?

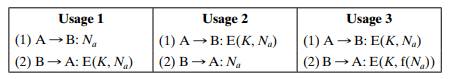
Step 1:

Federated identity management (FIM) is an agreement between several businesses or domains that enables users to log into all of their networks using the same identification information (digital identity). They are also referred to as "trust domains"

Step 2:

A user's identity can be connected between various independent identity management systems via federated identity. Users can swiftly switch between platforms while retaining security thanks to it.

There are three typical ways to use nonces as challenges. Suppose Na is a nonce generated by A, A and B share key K, and f() is a function (such as increment). The three usages are

[](https://files.transtutors.com/book/qimg/ab9bfec6-048e-40d2-ae2b-a3a874b2a818.png)

Describe situations for which each usage is appropriate.

Step 1:

All three have the same function. The vulnerability makes a difference.

Step 2:

In Usage 1, an attacker might compromise security by inflating Na and delaying B's response to launch a suppress-replay attack at a later time. The attacker could try to predict a feasible response in Usage 2, but if the nonces are random, this will fail. The messages in Usage 1 and 2 function in either way. This means that the response is E[K, N] if N is sent either way. Usage 3 encrypts the communication in both directions, and function f verifies that messages 1 and 2 are distinct from one another. Usage 3 is safer as a result.