What are the key elements of the PKIX model? Briefly describe each element.

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:

End entity:

A general word for any entity that may be recognized in the subject field of a public key infrastructure. It can refer to an end user, a device (such as a server or router), or any other entity. Typically, end entities use and/or support PKI-related services.

Certification authority(CA)

the certificate's issuer and, typically, its revocation list (CRLs).

Although they are frequently delegated to one or more registration authorities, it may also support a variety of administrative functions.

Registration authority(RA)

a component that is optional but has taken on some of the CA's administrative duties.

Although RA is frequently connected to the end entity registration process, it can also be helpful in a variety of other contexts.

CLR issuer:

A CA may assign a CLR issuer as an optional component to publish CRLs.

Explain the services provided by a federated identity management system.

Step 1:

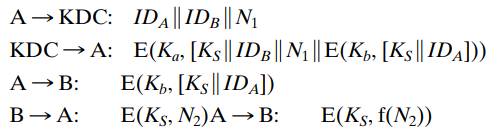
Federated identity management, sometimes referred to as federated SSO, is the process of building a trustworthy relationship between different businesses and outside parties, such as partners or application providers, that enables them to share identities and authenticate users across domains.

Step 2:

Federated identity enables authorized users to access many apps and domains with a single set of credentials. It links a user's identity across many identity management systems so they can access diverse applications securely and effectively.

When businesses use federated identity systems, users can access online applications, partner websites, Active Directory, and other applications without logging in separately.

Consider the following protocol:

[](https://files.transtutors.com/book/qimg/3c2bee46-2365-4420-ad47-be649d40ff0d.png)

a. Explain the protocol.

b. Can you think of a possible attack on this protocol? Explain how it can be done.

c. Mention a possible technique to get around the attack—not a detailed mechanism, just the basics of the idea.

Step 1:

This is the Needham Shroedar Protocol.

The Needham-Schroeder protocol is one of the two significant transport protocols created for use over an insecure network and both were proposed by Roger Needham and Michael Schroeder. These are referred to as The Needham-Schroeder Symmetric Key Protocol and employ symmetric encryption. It acts as the basis for the Kerberos protocol.

This protocol's objective is to establish a session key via a network between two parties, typically to protect further communication.

The Needham-Schroeder Public-Key Protocol is based on public-key cryptography. This protocol is intended to facilitate mutual authentication between two parties interacting across a network, despite the fact that its suggested form is insecure.

Step 2: Attack on Needham Shroedar Protocol.

The Needham-Schroeder authentication protocol has a flaw that we inherit. Consider that A connects to B. An enemy can continuously pass from A to B if they can record the "ticket" and somehow discover the related key.

The issue is that B is unable to determine whether the ticket is "new." B would be able to recognize re-used tickets if the ticket had a timestamp or some other form of the sequence number.

Step 3:

We use FDR to identify a protocol exploit that enables a hacker to pose as another agent. We modify the protocol, and then we demonstrate its security—at least for a small system—using FDR. Finally, we demonstrate a conclusion that says if this little system is secure, then any system of any size is also secure.