

Public Key Infrastructure (PKI) Certificate System

Lecture 8

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

- **Digital signature is a process that guarantees the contents of a message have not been altered in transit and gives a recipient reason to believe that the message was created by a known sender. However, a digital signature faces security threats. If the public key of the receiver is forged, the information sent is decrypted using the private key. The authenticity of a public key used by the receiver determines data confidentiality.**
- **One public key must be possessed by only one owner.**

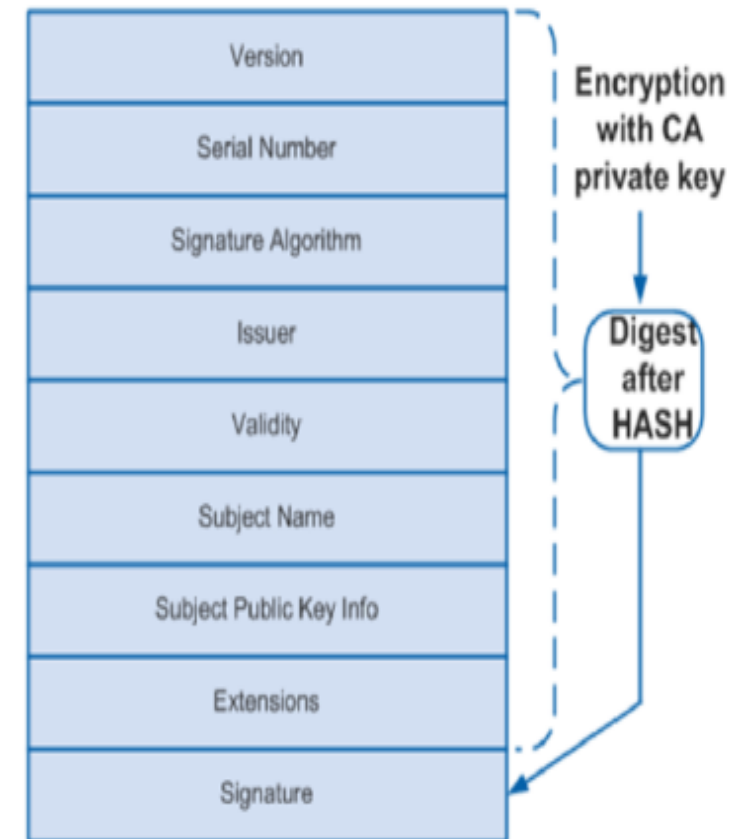
Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Describe the PKI certificate system architecture.**
 - ❑ **Master the implementation of the PKI certificate system.**

Digital Certificate

- A digital certificate (referred to as certificate), which is signed by the trusted certificate authority (CA) using digital signature, includes the certificate owner's public key and identity information.
- Certificate types:
 - ☐ Self-signed certificate
 - ☐ CA certificate
 - ☐ Local certificate
 - ☐ Local device certificate

- A simple digital certificate includes a public key, name, and digital signature of the CA.
- An X.509 v3 digital certificate contains mandatory information such as public key, name, and digital signature of the CA, and optional information such as validity period of the key, issuer (CA) name, and serial number.
- Meaning of each field in the digital certificate:
 - Version: version of X.509. Generally, the v3 (0x2) is used.
 - Serial Number: a positive and unique integer assigned by the issuer to the certificate. Each certificate is uniquely identified by the issuer name and the serial number.
 - Signature Algorithm: signature algorithm used by the issuer to sign the certificate.
 - Issuer: name of the device that has issued a certificate. It must be the same as the subject name in the digital certificate. Generally, the issuer name is the CA server's name.
 - Validity: time period during which a digital certificate is valid, including the start and end dates. Expired certificates are invalid.
 - Subject: name of the entity that possesses a digital certificate. In a self-signed certificate, the issuer name is the same as the subject name.
 - Subject Public Key Info: public key and the algorithm with which the key is generated.
 - Extensions: a sequence of optional fields such as key usage and CRL distributing address.
 - Signature: signature signed on a digital certificate by the issuer using the private key.



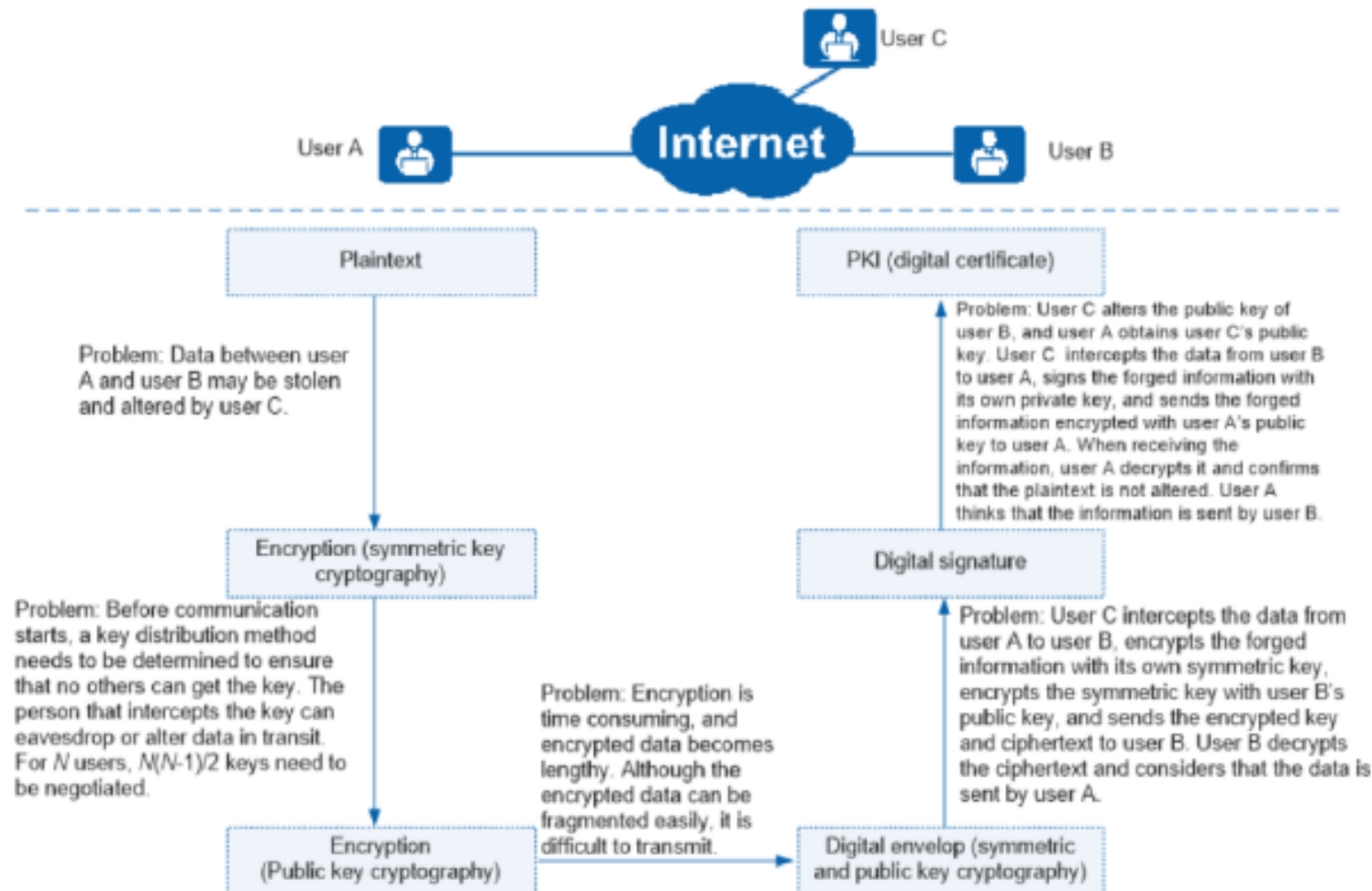
Certificate Format

- Three certificate formats are supported.

Format	Description
PKCS#12	Saves certificate files (with or without private keys) in binary format. Common file name extensions are .P12 and .PFX.
DER	Saves certificate files (without private keys) in binary format. Common file name extensions are .DER, .CER, and .CRT.
PEM	Saves certificate files (with or without private keys) in ASCII format. Common file name extensions are .PEM, .CER, and .CRT.

Chapter
08

Necessity of PKI

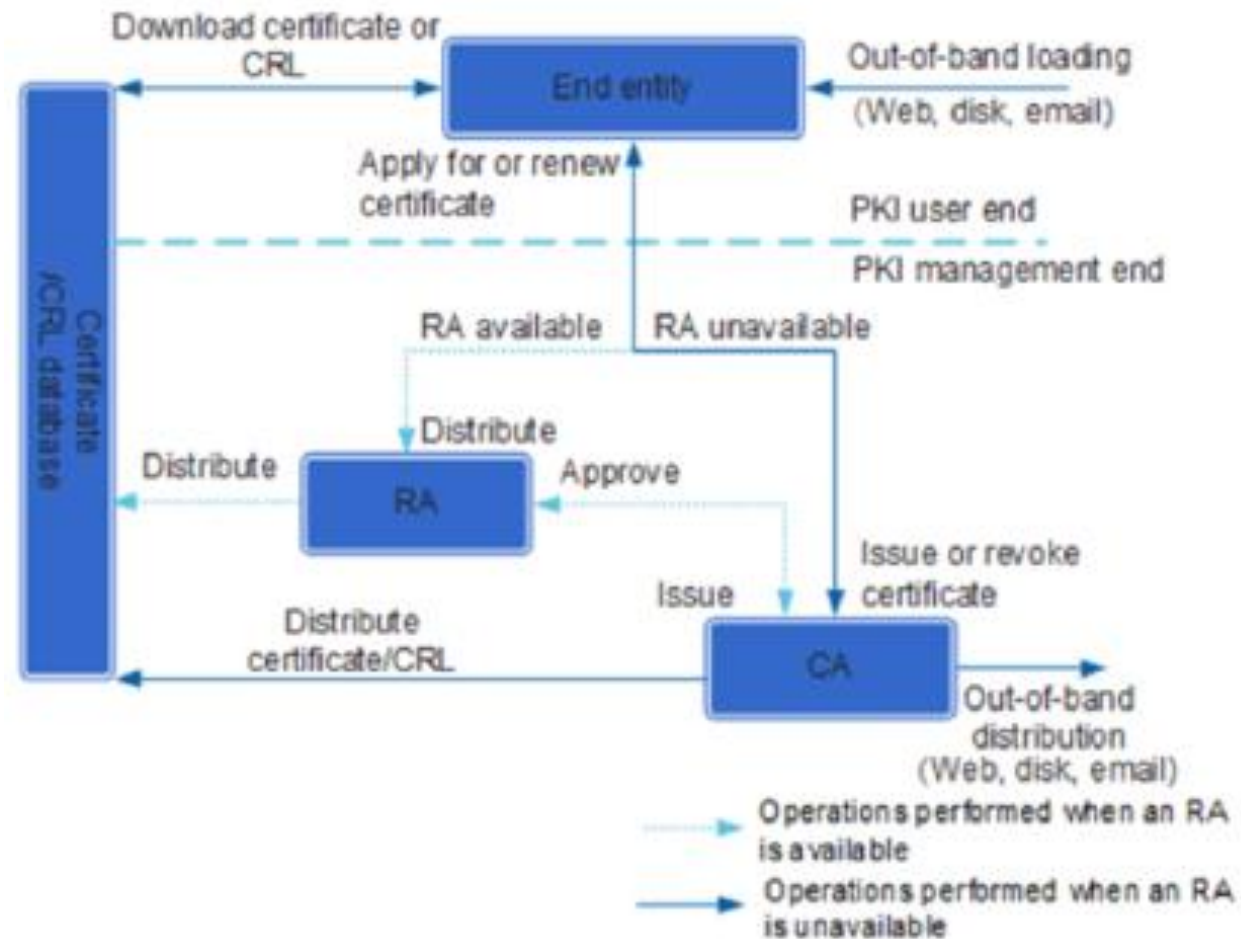


- PKI provides certificate management in compliance with certain standards. It uses public keys to provide security service for all network applications.
- PKI is the basis of e-commerce and the core of information security.
- As network and information technology develops, e-commerce is increasingly used and accepted. However, e-commerce has the following problems:
 - ❑ The transaction parties cannot verify the identities of each other.
 - ❑ Data may be eavesdropped and altered during transmission. Information is not secure.
 - ❑ No paper receipt is used in transaction, making arbitration difficult.
- To address these problems, PKI uses public keys to implement identity verification, confidentiality, data integrity, and non-repudiation of transactions. Therefore, PKI is widely used in network communication and transactions, especially by e-government and e-commerce.
- The core of PKI is digital certificate lifecycle management, including applying for, issuing, and using the digital certificates. During the lifecycle, PKI uses the symmetric key cryptographic, public key cryptographic, digital envelope, and digital signature.

PKI System Structure

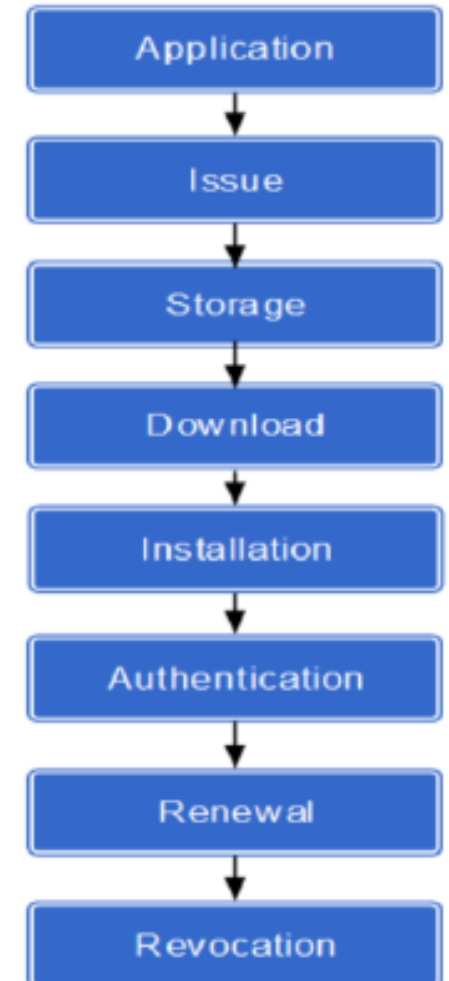
- A PKI system consists of an end entity, CA, Registration Authority (RA), and certificate/Certificate Revocation List (CRL) database.
- End entity: An end entity, or PKI entity, is the end user of PKI products or services. It can be an individual, an organization, a device (for example, a router or firewall), or process running on a computer.
- Certificate Authority (CA): The CA is the trusted entity that issues and manages digital certificates. The CA is an authoritative, trustworthy, and fair third-party organization. Generally, a CA is a server, for example, a server running Windows Server 2008.
- The CA on the top of the hierarchy is the root CA and the others are subordinate CAs.
- The root CA is the first CA (trust point) in the PKI system. It issues certificates to subordinate CAs, computers, users, and services. In most certificate-based applications, the root CA can be traced through the certificate chain. The root CA holds a self-signed certificate.
- A subordinate CA can only obtain a certificate from its upper-level CA. The upper-level CA can be the root CA or another subordinate CA authorized by the root CA to issue certificates. The upper-level CA is responsible for issuing and managing certificates of lower-level CAs, and the CAs at the bottom issue certificates to end entities. For example, CA 2 and CA 3 are subordinate CAs, holding the certificates issued by CA 1. CA 4, CA 5 and CA 6 are also subordinate CAs, holding the certificates issued by CA 2.

PKI System Structure

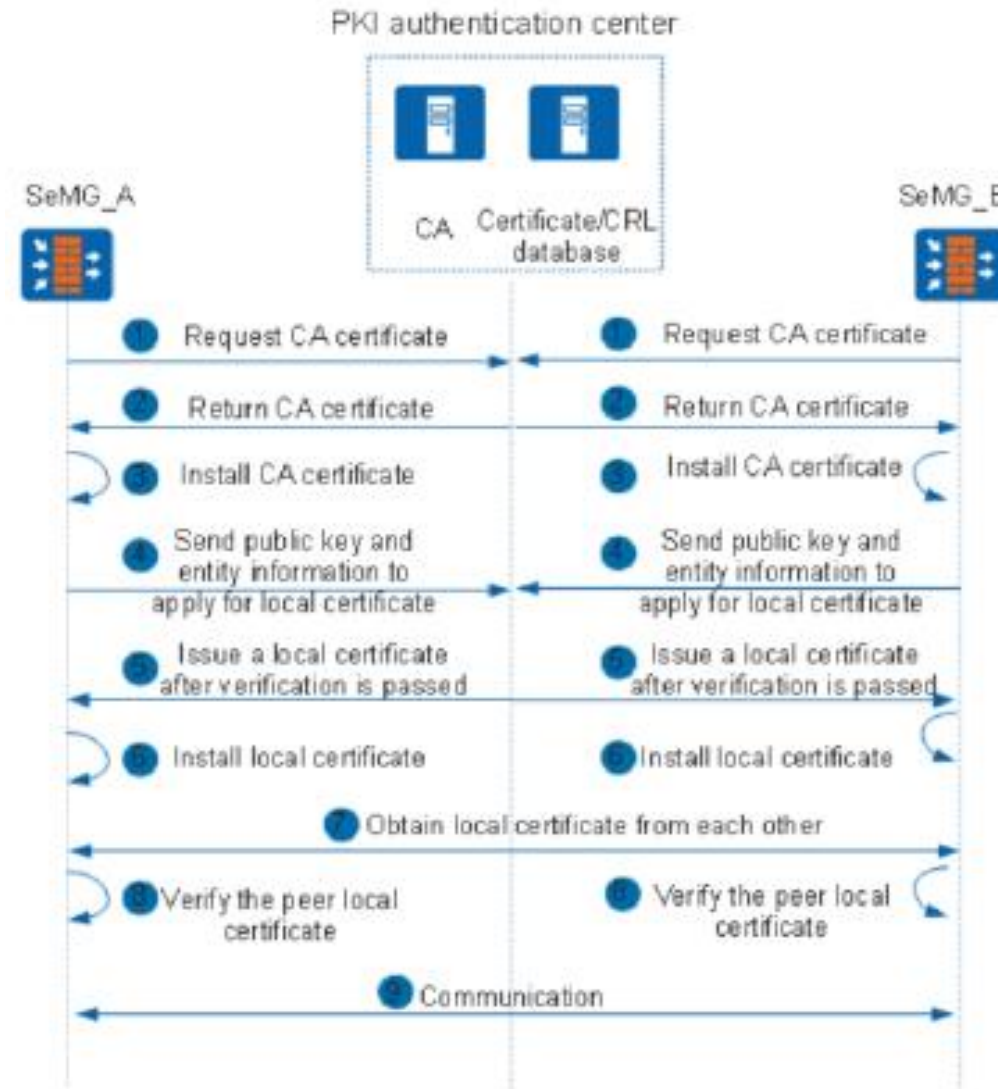


PKI Lifecycle

- PKI manages the entire lifecycle of local certificates, including application, issue, storage, download, installation, authentication, renewal, and revocation.
- Certificate application: Certificate application is certificate enrollment. It is a process in which an entity registers with a CA and obtains a certificate from the CA.
- Certificate issue: If an RA is available, the RA verifies the PKI entity's identity information when the PKI entity applies for a local certificate from CA. After the PKI entity passes verification, the RA sends the request to the CA. The CA generates a local certificate based on the public key and identity information of the PKI entity, and then returns the local certificate information to the RA. If no RA is available, the CA verifies the PKI entity.
- Certificate storage: After the CA generates a local certificate, the CA/RA distributes the certificate to the certificate/CRL database. Users can download or browse a directory of the certificates in the database.
- Certificate download: A PKI entity can download a local certificate, a CA/RA certificate, or a local certificate of another PKI entity from the CA server using SCEP, CMPv2, LDAP, HTTP, or out-of-band mode.
- Certificate installation: A downloaded certificate (a local certificate, CA/RA certificate, or certificate of another PKI entity) must be installed on the device (imported to the device memory); otherwise, the certificate does not take effect. A PKI entity obtains a CA certificate using SCEP and imports it to the device memory and then obtains a local certificate and imports it to the device memory.

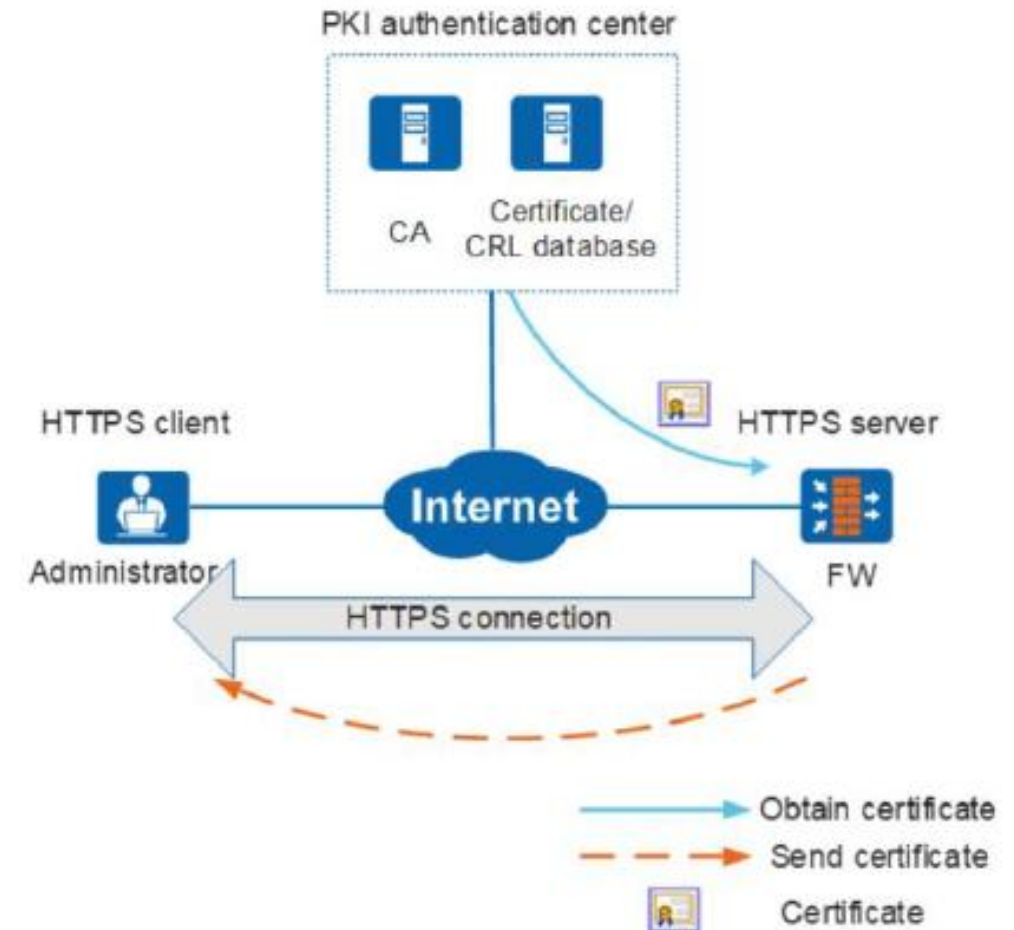


- On a PKI network, a PKI entity applies for a local certificate from the CA and the applicant device authenticates the certificate.



Logging In to Web Pages Using HTTPS

- Administrators can use HTTPS to securely log in to the WebUI of the HTTPS server for device management.
- To improve security of SSL connections, specify local certificates issued by the web browser-trusted CA for HTTPS clients on the devices. Then the web browser can verify local certificates, avoiding malicious attacks and ensuring secure login.

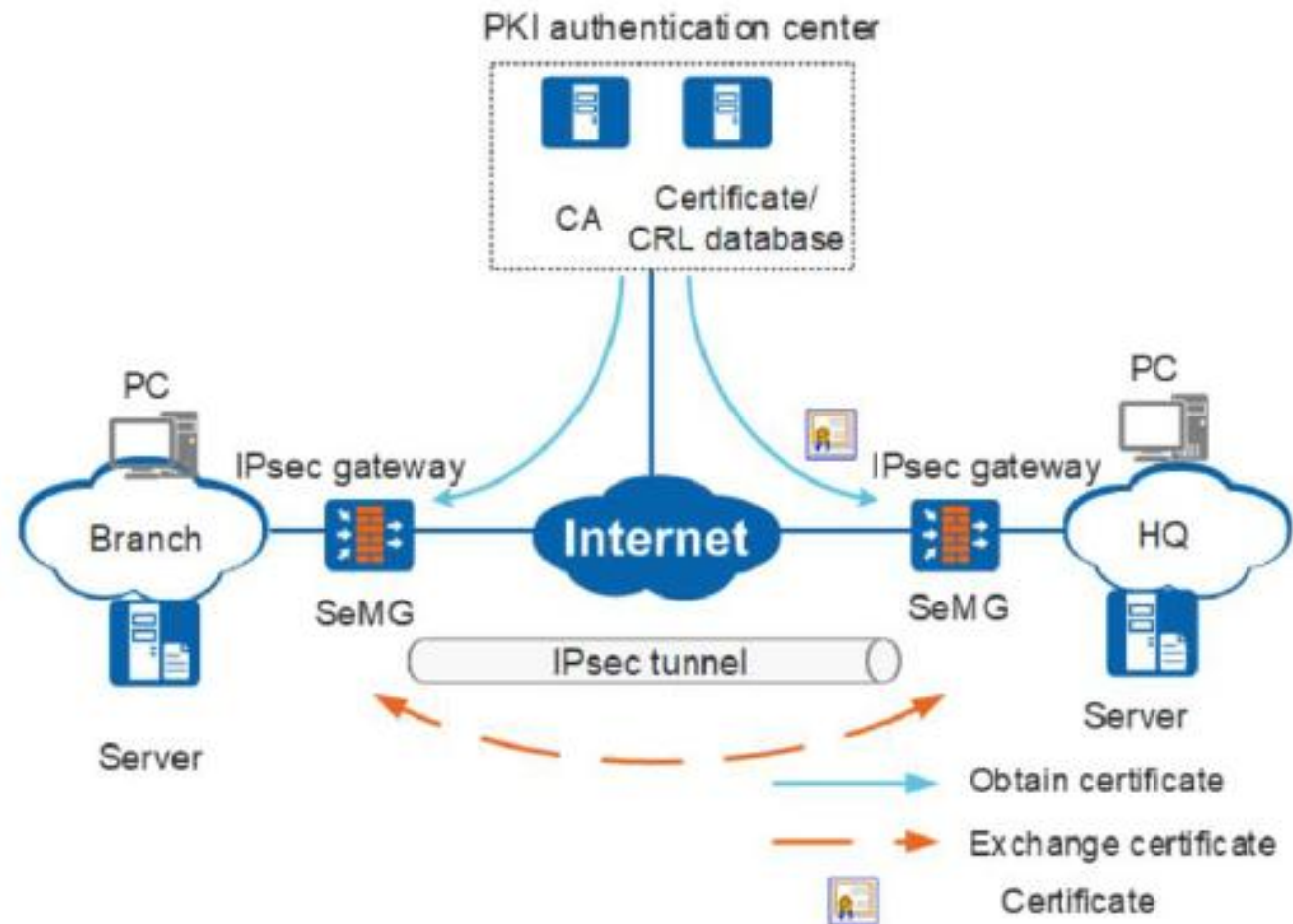


Chapter

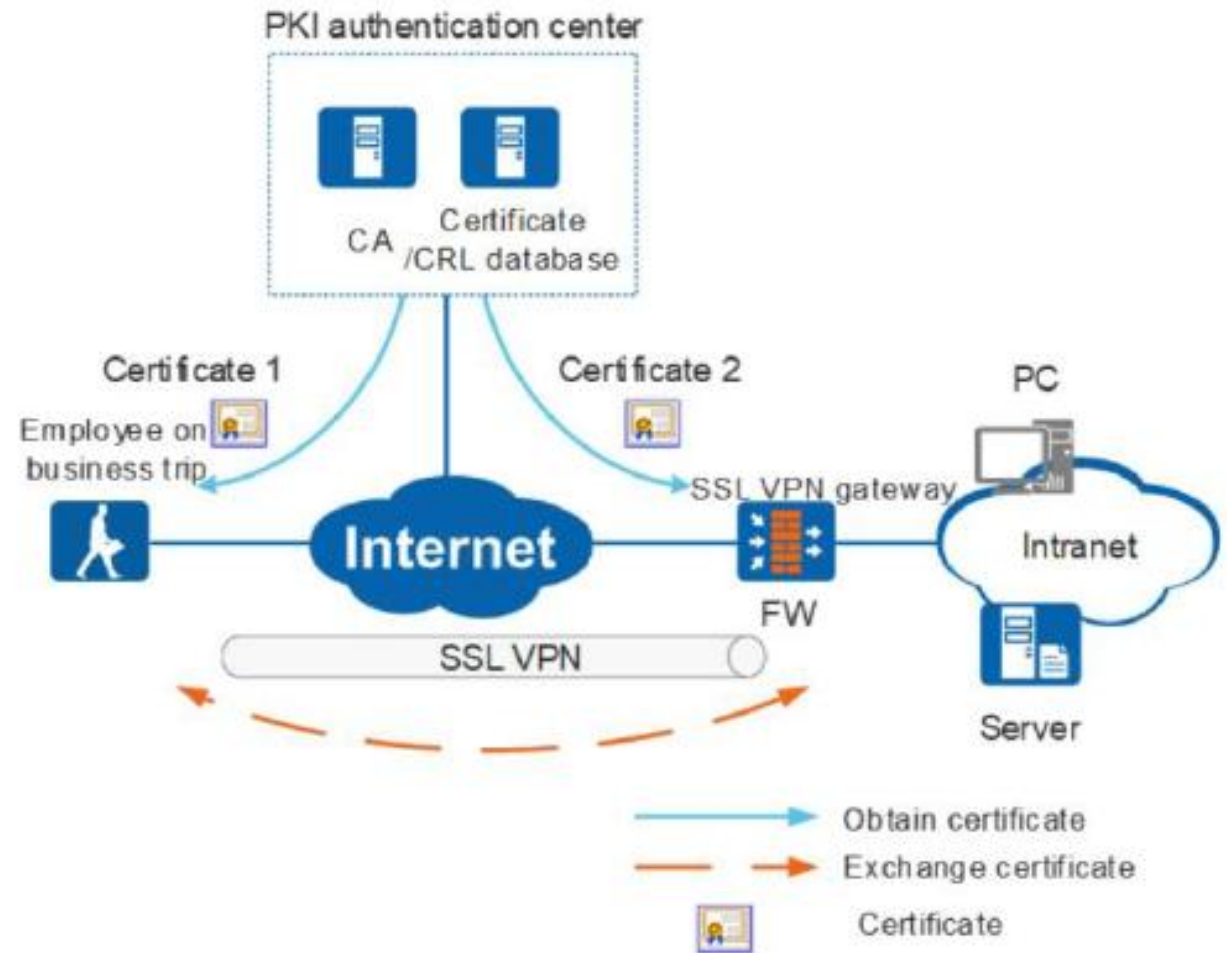
08

IPSec VPN

- The devices function as egress gateways of network A and network B. Intranet users of the two networks communicate through the Internet.
- To ensure data security over the Internet, the devices set up IPsec tunnels with the peer ends. Generally, IPsec uses the pre-shared key (PSK) to negotiate IPsec tunnels. However, using a PSK on a large network is not secure in PSK exchange and causes heavy configuration workloads. To address this problem, the devices can use PKI certificates to authenticate each other in IPsec tunnel setup.



- SSL VPN enables travelling employees to access intranets.
- They can enter usernames and passwords to access the intranets, but this method has low security. If the username and password of an employee are leaked, attackers may access the intranets, causing information leakage. To improve network access security, devices can authenticate users using PKI certificates.





Thank You