Workshop on Public Key Infrastructure and Red Hat Certificate System

Niranjan M.R, Huzaifa Sidhpurwala, Asha Akkiangady

Contents

1 Introduction to Public Key Cryptography

Before we start discussing about public key cryptography, we will in general discuss about how system communicate and what are the various threat models that are associated with the communication medium and what are the tools to overcome them.

Example1: The most common protocol used to communicate between 2 systems is TCP/IP. TCP/IP allows information to be sent from one system to another system directly or through many intermediate systems.

Below are some of the threat models associated with above communcation:

- **Eavesdropping:**

  Information remains intact, But it's privacy is compromised, For example: some one could learn credit card number, record a sensitive conversation or intercept a classified information.

- **Tampering:**

  Information in transit is changed or replaced and then sent to the recipient. For example: Some one could alter an order of goods or change a persons resume.

- **Impersonation:**

  Information passes to a person who poses as intended recipient. Impersonation can take 2 forms:

  - **Spoofing:**

    A person can pretend to be someone else, For example, a person can pretend to have email address *joe@example.net*, or computer can identify itself as a site called www.example.net, when it is not. This type of impersonation is called spoofing.

  - **Misrepresentation:**

    A person or organization can misrepresent itself, For example, suppose the site *www.example.net* pretends to be a furniture store when it's just a site which accepts payments but never sends any goods.

Example2: Consider Alice , Bob and attacker are the parties , where alice and bob want to communicate to each other and Attacker is a threat to the communication.

- Alice can send a postcard to bob to communicate, but this method is very weak as any random eavesdropper could read the postcard.

- Alice could write a letter and put in an envelope and send it to bob, but the attacker could open the envelope and read the letter, both confidentiality and integrity of the message is lost.

- Alice could seal the envelope with wax , but this method too is inefficient as Attacker could read the letter and seal it as it is without bob knowing that it was read by attacker

- Alice could write a letter and put it in a safe which has 2 keys and send one key before to Bob , and send the safe across to bob, this ensures confidentiality, integrity but practically this is not implementable. Considering the number of messages that has to be transferred , it's impractical to implement the mail safe method.

To mitigate above threat models, we will look in to cryptology as one of the tools of the trade.

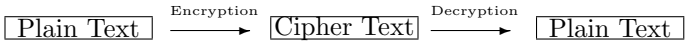
Cryptology: Cryptology is the theory of designing the various algorithms we use to provide security

Cryptography: Cryptography is the study of using these algorithms to secure systems and protocols.

1.1 Encryption

An encryption algorithm takes some data(called plaintext) and converts it to cipher-text under control of a key. cipher text contains random data which makes no sense without the key.

A key is a short random string (8-24 bytes):



When a message is encrypted and received , we cannot say if it's not tampered with. An encryption is strong when it can determine the number of possible keys. The attacker tries each key one at a time until he finds a key that produces a plausible decryption. The security of the algorithm should solely depend on the secrecy of the key. The algorithm should not need to be secret.

If the attacker knows the plaintext corresponding to the ciphertext it's called *"known plaintext attack"* .

An attack where attacker doesn't know the plaintext , it's called *"ciphertext-only attack"*. *Ex:* If the attacker knows that plaintext is ASCII , so any decryption which uses non-ascii characters must be using the wrong key.

1.1.1 Symmetric Encryption

When Sender and recipient share the same key(which must be kept secret) is referred to as *Symmetric Key Cryptograph* or also referred to as *Secret Key Cryptography* as opposed to *Public Key Cryptography*citation required?.

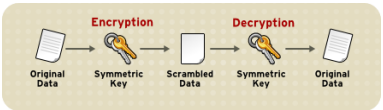


Figure 1: Symmetric Encryption

1.1.2 Assymetric Encryption

- First started in stanford university by Whitfield Diffie and Martin Hellman
- The most commonly used implementation of PKC are based on algorithm based on algorithm patented by RSA data security.

- Each public key is published & private key is kept secret. Data encrypted with public key can be decrypted only with private key.
- In general, to send encrypted data to someone, we encrypt with public key & the person encrypt receiving the encrypted data decrypts with private key
- Compared to symmetric key encryption, public key encryption requires more computation & therefore not always appropriate for large amounts of data
- It is possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data.

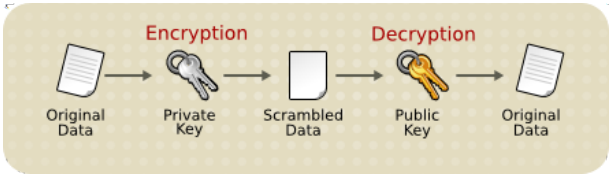


Figure 2: Assymetric Encryption

- Reverse of the above figure also happens i.e. encrypt with private key and decrypt with public-key. But not useful for sensitive information

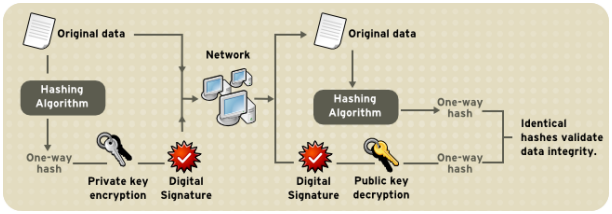


Figure 3: Digital Signature

- There's a problem with the above method, how would the parties get each other's public-key ? If we send the keys through electronically, then the attacker an tamper, while they are in transit to the receiver.
- When the 2 parties want to communicate, the attacker can intercept the keys & instead send his own key to each other, thus each party encrypts to him and & he re-encrypts it to the real recipient. This is called *man-in-the-middle attack*

1.2 Message Digest

A message digest is simply a function that takes as an input an arbitrary message and outputs a fixed length string which is characteristic of the message. The important property here is irreversibility. It's extremely difficult to compute a message from the given digest. Property of the message digest:

- For a digest to be secure, it must be difficult to generate any of the message that digests to the same value. You have to search a message space of proportional size of the digest in order to find a matching message text
- It should be difficult to produce 2 messages M and M' such that they have the same digest. This property is called collision-resistance. It turns out that the strength of any message digest against finding collision is only half the size of the digest., so a 128-bit digest is only 64 bits strong against collisions.

1.2.1 Message Authentication Code

Consider *Alice* and *Bob* share a key and Alice wants to send a message to *Bob*. The message can be encrypted, and send it across to *Bob*, but we are not sure that the encrypted message would be tampered and also not sure if *Alice* was the one who sent the encrypted message. So we use a new tool called *MAC* . *MAC* is a digest algorithm, but with a key, So the MAC is dependent on both the key and the message being MACed.

1.3 Algorithms

- **RSA**
  - RSA is the public-key algorithm widely used in Public-key Cryptography
  - Invented by Ron-Rivest, Adi Shamir and Len Adelman (RSA). Each user has a public-key and a private-key
  - The public-key can be freely distributed and the private-key must be kept secret.
  - Brief Explanation:
    * Generate 2 prime numbers (3, 17), call them p and q
    * n = modulus(p * q)
    * p and q are kept secret
    * Difficulty is in factoring m, so that we get p and q
    * Take another number "e" which is called public exponent, which is a prime number , it's usually small prime numers 3, 17 or 65537
    * Compute d = $e^{-1} mod((p-1)(q-1))$
    * Public Key = (e, n)
    * Private Key = (d, n)
    * Message M is encrypted with public key and decrypted with private key
    * RSA assumes that M is a number, So we need a convention to convert strings in to numbers.
- **DSA**
  - National Institute of standards and technology (NIST) published the Digital signature algorithm in the Digital signature standard.

- Compared to RSA where it can be used for both encryption and digital signature
- In DSA the signature generation is faster than signature verification

- **RC4**
  - RC4 is a stream cipher.
  - Assume we have a function (f) which produces 1 byte of data. This output is called keystream (ks)
  - The function (f) takes a encryption key as an input to generate keystream
  - Without the key we can't predict keystream
  - So combine each byte with one byte of plain text which is our ciphertext
  - C[i] denotes the ith unit of ciphertext
  - where a unit refers a 1 byte of data.
  - ks[i] refers the ith unit of keystream
  - M[i] refers to the ith unit of the message.
  - C[i] = ks[i] xor M[i]
  - m[i] = ks[i] xor C[i]
  - Disadvantages:
    - Assume we have used the same key to encrypt the Messages M and M'
    - If the attacker learns M and can compute ks by simply computing M xor C.
    - Once the attacker knows KS he can generate M'
  - RC4 was designed by Ron Rivest . RC4 is a variable key length cipher , with key can be anywhere between 8 to 2048 bytes long
  - SSL/TLS protocol use RC4 with 128-bit (16 bytes) key length
  - RC4 is extremely fast.

- **Block Ciphers**
  - **DES**
    - The data to be encrypted is processed in blocks of bytes (8 or 16).
    - Each possible plain text block corresponds to a row in the table
    - So to encrypt a block you find a column corresponding to the key, run down the table to find the row corresponding to the block you want to encrypt.
    - If the data is huge, it's very difficult to manage, so we define a function that does the computation
    - The idea is to simulate a random table
    - we have a key(k), and a data block . and we define 2 function E for encryption ,and D for decryption

    * C=E(K,M)
    * M=D(k,c)
    * When we have large messages , we do in Electronic code book mode.
        · Break the message up to block sized-chunks.
        · individually encrypt it using encryption algorithm
        · C[i]=E(k,M[i])
        · M[i]=D(K,C[i])
    * DES was desinged by IBM , it's patented but freely available
    * DES is a 64 block cipher with 56-bit key . The data is encrypted in blocks of 8 bytes and a key space of 56 bits.
    * DES is used with public-key techniques.
    * Disadvantages:
        · if M[i] and M[j] are same, then we get the same C[j] and C[k]. Attacker can get the pattern
        · Cipher block chaining mode, The encryption of each plain text block M[i] depends on cipher text of previous block C[i-1].
        · That can be accomplished by XORing previous Cipher text block C[i-1]] Xor M[i] before encryption
  - **3DES**
    * Run the DES algorithm 3 times.
    * It's used in Encrypt-Decrypt-Encrypt (EDE mode).
    * Message is encrypted with key-1, Decrypted with Key-2 and Encrypted with key-3.
    * 3DES is 3 times slower than DES.
  - **RC2**
    * RC2 is a block cipher invented by Ron Rivest,
    * RC2 is a variable-length cipher , with variable length key. It uses 64 bit block size.
  - **AES**
    * Advanced Encryption Standard uses a minimum of 128 bits and 3 key lengths, 128. 192 and 256 bits

- **Digest Algorithms**
  - The two most popular Digest Algorithms are MD5, which was designed by Ron Rivest and SHA-1 by NIST.
  - MD5 and SHA share a common ancestor MD4 also designed by Ron Rivest

1.4 Protocols

1.4.1 SSL

- Secure Socket Layer (SSL) is a protocol that provides a secure channel between machines

- It has facilities for protecting data in transit and identifying machine with which it is begin communicated
- Protocol is transparent , so it can be run on any protocol.
- SSL has gone through many versions and currently is culminating with the adoption by IETF as Transport Layer Security
- SSL was originally designed for world wide web , but also was intended as a unifying solution to all the other communications (web, mail, news traffic)
- The current version of SSL is tlsv2 which fixes a lot of security problems
- **Overview of SSL Protocol**
  - Primary goal of SSL is to provide privacy and reliability between 2 communicating applications
  - The protocol is composed of 2 layers : **Handshake protocol** and **record protocol**
  - In brief Handshake protocol provides
    - allows server & client to authenticate to each other
    - Negotiate encryption algorithm or Cryptography keys.
  - Record protocol provides:
    - Confidentiality
    - Authenticity
    - replay protection
- **Handshake Protocol**
  - Client sends a list of algorithms it's willing to support along with a random number used as input to a key generation proces
  - Server chooses out of that list and sends it back along with a certificate containing servers public-key.
  - certificate also provides the server's identity for authentication purpose and the server supplies a random number which is used as a part of key generation process
  - Client verifies the servers certificate and extracts the server's public-key from the certificate
  - Client then generates a random secret called *pre_master_secret* and encrypts this with server's public-key
  - Client sends this encrypted *pre_master_secret* to the server
  - Client and the Server independently compute the encryption and MAC keys from *the pre_master_secret* and client and server's random values
  - Client sends a MAC of all the handshake messages to the server
  - The server sends a MAC of all the handshake messages to the client
  -

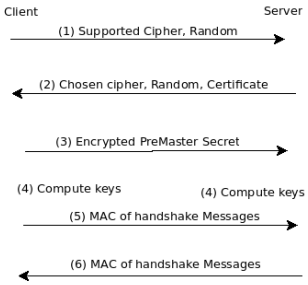


Figure 4: SSL Handshake

- Step:1 corresponds to single SSL Handshake message, Client Hello
- Step:2 corresponds to SSL Handshake messages
  - First is a ServerHello Algorithm preference, Certificate
  - Send ServerHelloDone
- Step3 correponds to ClientKeyExchange
- Step 5 and 6 correspond to the finished message. The Finished message is the first message that's the protected using Just-Negotiated algorithms.
- To protect the handshake from tampering, the content of the message is MAC of all the previous handshake messages

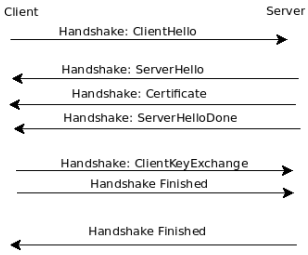


Figure 5: SSL Handshake

-
- **Resuming Session**
  - client sends a clientHello with a Session-ID of the session to be resumed.
  - server check it's session cache for a match
  - If the match is found & the server is willing to re-establish the connection under specified session state , it will send a Server-Hello with same session-ID
  - At this point both client and server must send change Cipher spec messages & proceed directly to finished messages
  - There is no exchange of certificates here.
  - Once the re-establishment is complete the client & server may begin exchange of application data

    * If the Session-ID match is not found the server generates a new session-ID & the client and Server have to perform a full handshake

- **SSL Record Protcol**
  - The actual data transfer is accomplished by SSL Record Protocol
  - Record Protocol works by breaking up the data stream to be transmitted in to a series of fragments, each of which is independently protected and transmitted.
  - On the receiving end , each record is independently decrypted and verified.
  - Before transmission , a MAC is computed on each record , This MAC is transferred along with the record
  - The concatenated data and MAC are encrypted to form encrypted Payload. We attach a header to that encrypted payload which we refer to as a record

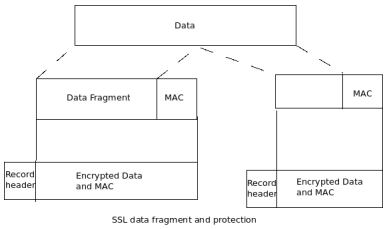


Figure 6: ssl data fragment and protection

  -
  - The record header provides the information for the other end to interpret the record. It contains:
    * Content Type (Application data, alert messages, handshake message, change cipher spec)
    * length (how many bytes to read off wire)
    * SSL Version
  - The *change_cipher_spec* message indicates a change in encryption and authentication of records
  - Once the handshake is completed a new set of keys is negotiated, *change_cipher_spec* record is sent to indicate that those keys will now be used.

1.5 Exercises

2 Introduction to Public Key Infrastructure

Below is a simplified architectural model of Public Key Infrastructure using X.509 (PKIX) Specifications

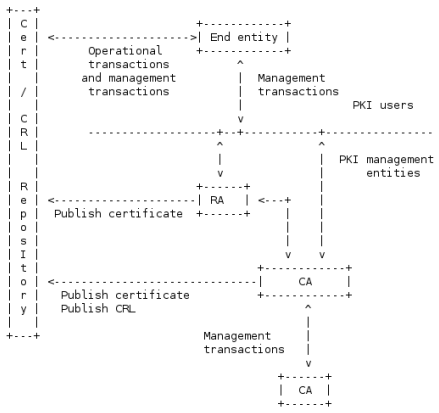


Figure 7: PKI Architectural Model

2.1 Common Terms used in PKI

- End Entiy: User of the PKI certificates and/or end user system that is the subject of a certificate
- CA: Certificate Authority
- RA: Registration Authority, Optional System to which CA delegates certain management functions
- CRL issuers: A system that generates CRL
- repository: a system or collection of distributed systems that stores certificates and CRLs and services as a means of distributing these certificates and CRLs to end entities

2.2 Detailed look on certificate/CRL

2.2.1 Certificates

- Certificates are data structures that bind public key values to the subject. This binding is asserted by a trusted Certificate Authority.
- X.509 defines the standard certificate format and v3 is the latest version.
- Internet Privacy Enhanced Mail(PEM) RFC 1421 and 1422 also include specifications for PKI based on X.509 certs.
- Types of Certificates:
  - End-Entity
  - CA
- RFC 1422 defines hierarchial structure of CA's and there are three types of PEM CA

  - IPRA: Internet Policy Registration Authority , acts as Root of Certificate authority. IPRA operates under Internet Society Organization
  - PCA: Policy Certificae Authority ,(Verisign, Digicert, etc) signed by IPRA
  - CA: Certificate Authorities signed by PCA (Organizational CA's)

- Policies used by CA:
  - IPRA certifies only PCA and not CA's or users cert
  - IPRA will make sure that the DN of the PCA is unique and will not certificate PCA's with similar DN
  - Certificates should not be issued to distinct entities under the same distinguished Name.
  - IPRA should not certifiy two PCA's with same DN
  - PCA's should not certify two CA's with same DN
  - CA's are expected to sign certificates only if the subject DN in the certificates is subordinate to the issuer CA DN.

- Types of Certificate Authorities
  - Cross-Certs: Where Issuer and Subject are different
  - Self-Issue: Where Issuer and Subject are same
    * Self-Signed: Where key bound in to the certificate is same as the key used to sgin the certificate

2.2.2 Basic Certificate Fields

- Version:
  - Describes the version of encoded certificate.
  - if extensions are used: **0x2(3)**
  - if extensions are not used but UniqueIdentifier is used: **0x1(2)**
  - if only basic fields are there: **0x0(1)**
  - Values: **0x2(3), 0x1(2), 0x0(1)**

- Serial Number:
  - Positive integer assigned by CA to each certificate
  - It must be unique for each Certificate given by CA
  - Can contain long integers (up to 20 Octets)
  - Values: Integers:
    * **16694152257348400000**
    * **0xe7ad8b07558a1727**
    * **cd:ba:7f:56:f0:df:e4:bc:54:fe:22:ac:b3:72:aa:55**

- Signature:
  - Algorithm used by **CA** to sign the certificate
  - Value:
    - **md2WithRSAEncryption**
    - **sha1WithRSAEncryption**
- Issuer:
  - Identifies the entity that has signed and issued the certificate
  - **MUST** contain non-empty Distinguished Names
  - Names should confirm to X.501 standard
  - Generally contains Country, Organization, Common name, Serial-Number, province, State, title, Surname, Generation Qualifier(Jr, Sr).
  - Values:
    - **C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority**
    - **C=DE, ST=Bayern, L=Muenchen, O=Whatever it is, CN=IO::Socket::SSL Demo CA**
    - **C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority**
- Validity:
  - The time interval during which the CA warrants that it will maintain status of the certificate
  - Consists sequence of 2 dates
    - Date on which certificate validity begins
    - Date on which certificate validity ends
  - Validity period of a certificate is period from notBefore to notAfter(inclusive)
  - Values:
    - **Not Before: Jan 29 00:00:00 1996 GMT**
    - **Not After : Aug 1 23:59:59 2028 GMT**
    - Special Note:
      - Devices are given certificates where there is no expiration date
      - Value:
      - Certificate is to be used for entire lifetime of the device **Not After: 99991231235959Z.(represented in Generalized Time)**
- Subject:
  - Identifies the entry associated with public key stored in the subject public key field

  - If the subject is CA then it should be populated with same data as issuer
  - Names should confirm to X.501
  - Values:
    * **C=US, ST=North Carolina, O=Fedora Project, OU=Fedora User Cert, CN=mrniranjan/emailAddress=niranjan@ashoo.in**

- Subject Public key Info:
  - This field is used to carry public key and identify the algorithm with which the key is used (RSA, DSA)
  - Supported Cryptographic Algorithms:
    * **Rivest-Shamir-Adelman (RSA)**
    * **Digital Signature Algorithm (DSA)**
    * **Diffie-Hellman (DH)**
    * **Elliptic Curve Digital Signature Algorithm (ECDSA)**
    * **Key Encryption Algorithm (KEA)**
    * **Elliptic Curve Diffie-Hellman (ECDH)**

2.2.3 Extensions

- This field only appears in v3 Certs
- This contains sequence of one or more Certificate Extensions
- Extensions provides method for associating additional attributes with public keys
- Managing relationship between CA's
- Can carry private extensions to carry information unique to their community
- Each Extension is either Critical / Non Critical
- Each Extension includes OID and ASN.1 DER (OCTET)
  - Example: DE:65:01:16:19:2E:51:E0:9A:51:1A:37:50:94:7D:39:29:2A:42:2C
- There cannot be duplicates of Extensions
- Default CRITICAL value is false
- If the Certificate is CA , then they should have below Extensions
  - Basic Key Identifier
  - Authoritative key Identifier
  - Basic Constraints
- **Authority Key Identifier:**
  - Provides a means of identifying the public key corresponding to the private key used to sign the certificate

- This is required if the issuer has multiple signing keys
- If the CA certificate is self signed Authority key identifier is skipped
- Authority key Identifier helps in identifying the issuer certificate.
- Values:
  - **keyid:48:E6:68:F9:2B:D2:B2:95:D7:47:D8:23:20:10:4F:33:98:90:9F:D4**

- **Subject Key Identifier:**
  - Provides a means of identifying certificates that contain a particular public key
  - This extension is must for CA certificates
  - The value placed in this is same as Authority Key Identifier
  - For End-entity Certificates, this extension provides a means for identifying certificates containing particular key used in application
  - Value:
    - **48:E6:68:F9:2B:D2:B2:95:D7:47:D8:23:20:10:4F:33:98:90:9F:D4**

- **Key Usage:**
  - Defines the purpose of the key contained in the certificate
  - This extension is used to restrict the usage of the key to be used for purpose other than what is defined in Key Usage
    - **digitalSignature**
      - Public key should be used only to verify signatures on objects other than Public key certificates/CRL
    - **nonRepudiation/contentCommitment**
      - subject Public key is used to verify digital signatures other than signatures on public key(CRL)
      - used to provide nonRepudiation Service that protects against signing entity falsely denying any public action
    - **keyEncipherment**
      - Public key is used for enciphering private key or secret keys ,
      - Is used for encrypting symmetric content-decryption key or an assymetric private key
    - **dataEncipherment**
      - is used for enciphering the raw data without the use any cipher (very rarely used)
    - **keyAgreement**
      - is used for key Agreement,
      - when used Deffie-Hellman key is to be used for key management
    - **keyCertSign**
      - Public key is used for verifying the signatures on public keys , if this is true then

* **cRLSign**
  - when the subject public key is used for verifying signatures of CRL
* **encipherOnly**
  - subject's public key may be used only for enciphering data while performing key agreement
* **decipherOnly**
  - subject's public key may be used only for deciphering data while performing key agreement
* Important Note:

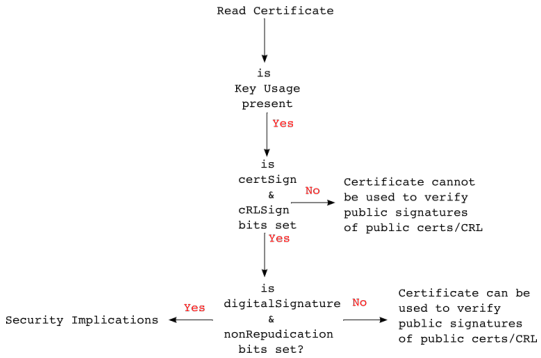


Figure 8: Key Usage restrictions

.

- **Certificate Policies**
  - Contains sequence of one or more policy information terms each of which consits of OID, optional Queries
  - OID Should not appear more than once
  - for End-entity policy information terms indicate the policy under which the certificate has been issued and purposes for which the certificate must be used
  - For CA the policy limits the policies for certificate paths that include this certificate
  - if CA does not want to limit the set of policies for certification paths then it may assert **anyPolicy** with value **2.5.29.32.0**
  - Policy Qualifiers:
    * CPSNotice: Points URL to *certificate practice statement* document that describes the policy under which the subject was issued
    * userNotice: text that describes the policy(not more than 200 characters)
- **Policy Mappings**
  - This extension is used by CA certificates

- Lists one or more pairs of OID, which indicate that the corresponding policies of one CA are equivalent to policies of another CA [used in context of Cross pair certificates]
- **OID: 2.5.29.33**

- **Subject Alternative Name**
  - Allows alternate names to be bound to subject of the certificate.
  - The names specified in subjectAltName may be included in addition to or in place of the identity in the subject field of the certificate
  - Defined subject names used:
    * rfc822Name: IA5String
    * otherName: OtherName
    * dNSName: IA5String
    * directoryName: Name
    * URI: IA5string
    * iPAddress: OCTET String
    * UniformResourceIdentifier: IA5String

- **Issuer Alternative Name**
  - Allows alternate names to be bound to certificate issuer
  - Issuer alternative names are not processed as part of certification path validation
  - Issuer Alternative name extension when present should be non-critical

- **Subject Directory Attributes**
  - This extension is used to convey identification attributes of the subject
  - Value:
    * nationality of the subject

- **Basic Constraints**
  - This extension identifies whether the subject of the certificate is CA ?
  - It also identifies Maximum depth of valid certification paths that include this certificate
  - Values:
    * cA: (boolean): indicates whether certificate is CA cert
    * pathLenConstraint: applicable if cA boolean is true. if prsent asserts keyCertSign bit.
    * It gives maximum number of non-self-issued intermediate Certificates that may follows this certificate in a valid certification path. The last cert is End-entity certificate
    * Ex: PathLength is 2:
      · RootCA - EE Cert

- RootCA - subca1-EE Cert
- RootCA - subca1-subca2-EE Cert
- RootCA - subca1-subca2-subca3-EE Cert

- **Name Constraints**
  - Used only in CA certificate
  - Specifies name space within which all subject names in subsequent certificates ina certification path MUST be located.
  - Restrictions apply to Subject Dishtinguished Name and subject alternative names.
  - Restrictions do not apply for self-issued certs
  - Restrictions are defined in terms of permitted or excluded name subtrees
  - if name matches a restricted excluded subtrees, it 's invalid eventhough the name matches permittedsubtrees.
  - Examples:
    * URI: constraint applies to host part of the name
    * emailAddress: Example .example.org [indicates all emails with domain .example.com]
    * DNS : pki.example.org [www.host1.pki.example.org would satisfy but host1.example.org will not]
    * directoryName: Compares the DN attributes.

- **Policy Constraints**
  - policy constraints extension can be used in certificates issued to CAs.
  - Asserts policy related constraints
    * inhibitPolicyMapping: if present policy mapping is to be inhibited while processing subsequent certificates
    * requireExplicitPolicy: if present indicates subsequent certificates need to include an acceptable policy identifier

- **Extended Key Usage**:
  - This extension is used to indicate one or more purposes for which certificates public key can be used:
    * id-kp-serverAuth: TLS WWW server authentication
    * id-kp-clientAuth: TLS WWW client authentication
    * id-kp-codeSigning: Signing of downloadable executable code
    * id-kp-emailProtection: Email protection
    * id-kp-timeStamping: Binding the hash of an object to a time
    * id-kp-OCSPSigning: Signing OCSP responses

- **CRL Distribution Points**
  - cRLDistributionPoints extension is combination:

    - distributionPoint
    - reasons
    - cRLIssuer

- **Authority Information Access**
  - Indicates how to access information and services for the issuer of the certificate in which the extension appears
  - Information and services include, On-line validation services, CA policy data
  - This extension is added in both EE and CA cert
- **Subject Information Access**
  - This extension indicates how to access information and services for the subject of the certificate in which the extension appears
  - If the subject is CA, informaiton and services may include certificate validation and CA policy data.
  - If the subject is EE, information describes the type of services offerred and how to access them

2.2.4 Revocation

When a certificate is issued, it is expected to be used for it's entire validity period. Due to various circumstances, certificate can be invalidated like:

- Change of name
- Change of association with subject and CA (Employee left)
- Compromise or private key
- CA wants to revoke the certificate
- X.509 defines one method of revoking certificates, where CA periodically issues a signed data structure called Certificate revocation list (CRL).
- CRL is a time-stamped list identifying revoked certificates that is signed by CA or CRL issuer.
- This list is freely available through public repositories
- It is expected that the certificate system user not only verifies certificate validity, signature but also aquires latest CRL from public repositories and check against CRL
- CRL's are issued periodically (hourly, daily or weekly).
- CRLissuers or CA issue CRL
- CAs publish CRLs to provide status information about the certificates they issued
- CA may delegate this responsibility to another trusted authority

- Details of CRL
  - Each CRL ahas particular scope
  - CRL scope is the ste of certificates that could appear in a given CRL
  - Examples:
    * all certificates issued by CA x
    * all CA certificates that has been revoked by key compromise or CA compromise
    * set of certificates base on arbitrary local information (all certificate issued to employees at location X)
  - CRL list all **unexpired** certificates, within it's scope that have been revoked for one or other reason
  - If the scope of the CRL includes one or more certificates issued by an entity other the CRL issuer it's called **indirect CRL**
  - CRL issuer may also generate delta CRL.
  - **Delta CRL** only lists those certificates whose revocation status has changed since the issuance of referenced complete CRL.
  - Referenced complete CRL is called **complete CRL**
  - Scope of the delta crl should be same as base CRL that it references
  - When CRL's are issued CRLs must be version 2 CRLs.

2.2.5 CRL Fields

- **Version** All CRLs must be Version 2 CRLs
- **Signature Algorithm**
  - Contains algorithm identifier for the algorithm used by the CRL issuer to sign the certificatesList
  - Values:
    * **SHA256withRSA - 1.2.840.113549.1.1.11**
- **Issuer Name**
  - Issuer Name identifies the entity that has signed and issued the CRL
  - Alternative name forms may also appear in the issuerAltName Extension
  - The issuer must contain a non-empty X.500 DN.
- **This Update**
  - This field indicates th issue date of this CRL.
  - Example:
    * **This Update: Sunday, January 17, 2016 8:06:03 AM IST Asia/Kolkata**
- **Next Update**

- This field indicates the date by which the next CRL will be issued.
- The next CRL may be issued before the indicated date, but it will not be issued later than indicated date.
- CRL issuers(CA) **SHOULD** issue CRLs with nextUpdate time equal to or later thean all previous CRLs.

- **Revoked Certificates**
  - Contains list of certificates revoked by CA
  - Certificates revoked by CA are uniquely identified by their certificate serial Number.
  - Date on which revocation occurred is specified.

2.2.6 CRL Extensions

- **Authority Key Identifier**
  - This extension provides a means of identifying the public key correspondign to the private key used to sign the CRL. This identifier can be based on either the key identifier or issuer's name and serial number.
  - Example:
    * Authority Key Identifier Example:

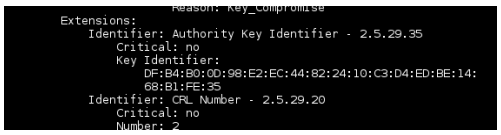


Figure 9: CRL Authority Key identifier

- **Issuer Alternative Name**
  - This extension allows additional identities to be associated with the issuer or CRL.

- **CRL Number**
  - This is a non critical extension that specifies sequence number for a given CRL scope and issuer.
  - This extension allows users to determine if a particular CRL supersedes another CRL.
  - if a CRL issuer generates delta CRLs in addition to complete CRLs for a given scope, the complete CRLs and delta CRLs must share one numbering sequence.

- **Delta CRL Indicator**
  - Delta CRL indicator is a critical CRL extension that identifies a CRL beging a delta CRL.

- Delta CRLs contain updates to the revocation information previously distributed, rather than all the information that would appear in complete CRL.
- This helps in reducing network load and processing time in certain environments
- Example:

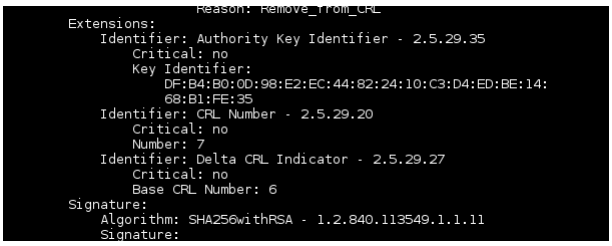


Figure 10: Delta CRL Indicator Extension

*

- **Issuing Distribution Point**
  - This is a critical CRL extension that identifies the CRL distribution point and scope for a particular CRL.
  - It indicates whether CRL covers revocation of EE Certificates only, CA certificates etc.
  - Example:

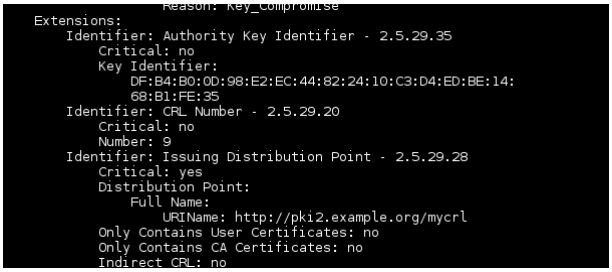


Figure 11: Issuing Distribution Point extension

*

2.3 Exercises

3 Red Hat Certificate System

3.1 Certificate Manager

3.1.1 Introduction

Certificate Manager is the first subsystem that needs to be configured in PKI Environment, Certificate Manager can be configured as RootCA, Subordinate CA

3.1.2 Installation

- RPM: **pki-ca**
- configuration: CA subsystem is configured using utility **pkispawn**.

  pkispawn provides both interactive configuration or silent configuration by reading a configuration file.

  pkispawn first reads **default.cfg** first and gets other deployment specific information through interactive method or through batch mode by reading a file.

  pkispawn then passes this information to a java servlet which performs the configuration.

Figure 12: Configuring CA subsystem using pkispawn

3.1.3 Key Features

- CA subsystem issues, renews, revokes Certificates, generates Certificat Revocation lists
- Publishes Certificates/CRL in form of files or can publish to LDAP or OCSP responder
- CA also has an inbuilt OCSP responder enabling OCSP-Compliant clients to query CA about revocation status of Certificate

- Some CA's can delegate some of it's responsibility to another Subordinate CA

3.1.4 Architecture

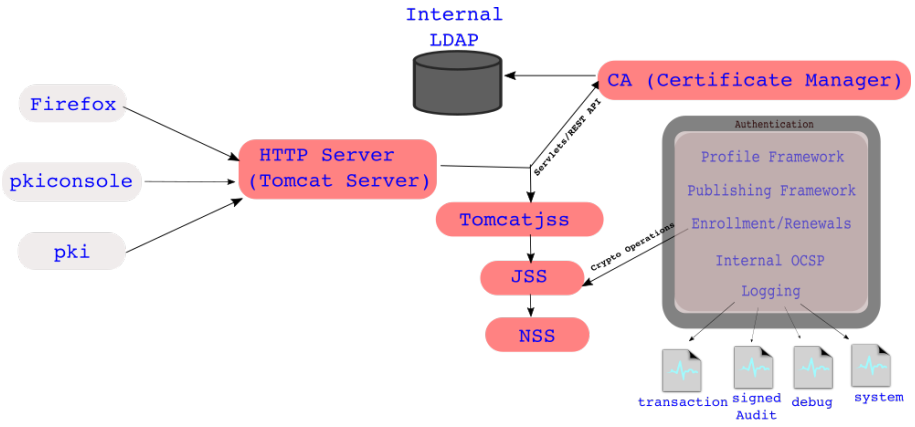


Figure 13: CA Subsystem Architecture

3.1.5 Interfaces

- End User Interface(Browser/CLI)
- Agent Interface(Browser/CLI)
- Admin interface(java console)

3.1.6 Features

- Enrollment:

  End user Enrolls in the PKI infrastructure by submitting a Enrollment(certificate) request through End Entity Interface. This request can be submitted through 2 Methods:

  - Browser
  - CLI

  There can be different kinds of Enrollment(Certificate) Request:

  - Request for User, Server, SMIME, Dual Cert,.. certificate
  - Request certificate if authentication through ldap, pin, cert etc.

  Based on the above types, there are different certificate profiles associated with it. When end-entity(user) enrolls a certificate following events occur:

- The End-entity provides the information in one of the enrollment forms and submits a request
- The enrollment forms triggers the creation of public-key and private-key or dual-key pairs
- The End-entity provides authentication credentials before submitting the request, depending on the authentication type. This can be LDAP authentication, PIN-based authentication or certificate-based authentication.
- The request is submitted either to an agent-approved enrollment process or an automated process.
  * Agent-approved process requires no end-entity authentication, sends the request to the request queue in the agent-services interface.
  * Automatic notification can be setup so an email can be sent to an agent any time a request appears in the queue
  * The automated process, which involves end-entity authentication,process the certificate as soon as the end-entity successfully authenticates
- This form collects information about the end entity from the LDAP directory when the form is submitted
- The profile associated with form determine the aspects of certificate that is issued. Depending upon the certificate profile the request is evaluated to determine if the request meets the constraints set.
- The Certificate request is either rejected because it did not meet the certificate profile or authentication requirement, or a certificate is issued
- The certificate is delivered to end-entity through HTML interface or email or certificate can be retrieved through Agents interface by serial number or request-ID.
- The new certificate is stored in Certificate Managers internal database.

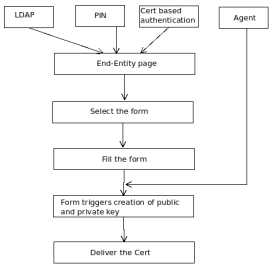


Figure 14: Certificate Enrollment

- Profiles:

  Profile determine the content of a certificate. Certificate manager provides customizable framework to apply policies for incoming certificate requests and to control the input requests types and output certificate types

Certificate Profile define the following:

- Authentication Method
- Authorization Method
- Certificate content
- Constraints for the values of content
- Contents of input
- Output

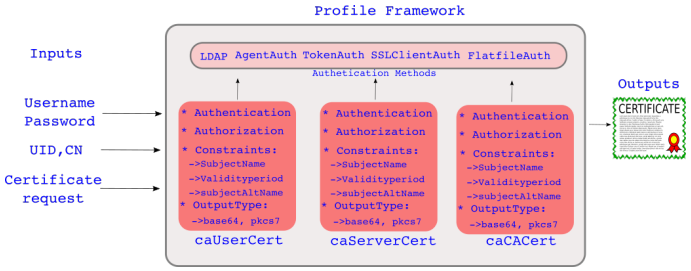


Figure 15: Certificate Profile Architecture

Profile Workflow:

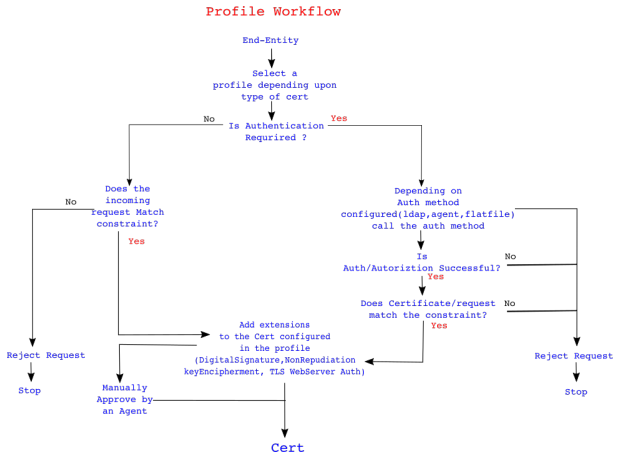


Figure 16: Certificate Profiles Workflow

Each profile are defined in **.cfg** file located at **/var/lib/instance_name/profiles/ca** directory

Example **caUserCert** Profile:

The first part of the profile is the description and specifies whether profile is enabled or disabled, if enabled who enabled it.

The second part of the profile describes the inputs:

- KeyGenInputImpl: specifies the key pair generation during the request submission, This provides if the request should be of type CRMF/PKCS10, also provides dropdown specifying the key size.

Figure 17: Profile Description

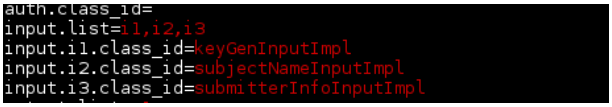


Figure 18: Profile inputs

– subjectNameInputImpl: specifies the subject Distinguished Name(DN) to be used in the cert. The subject DN can be constructed from *UID, Email, Common Name, Organizational Unit, Country*
– submitterInfoImpl: This input specifies three fields: *Requester Name, Requester email, Requester phone*

Figure 19: Profile output

Third part of the profile is output,

– certOutputImpl: The certificate output format *base64, pkcs7, pret-typrint*

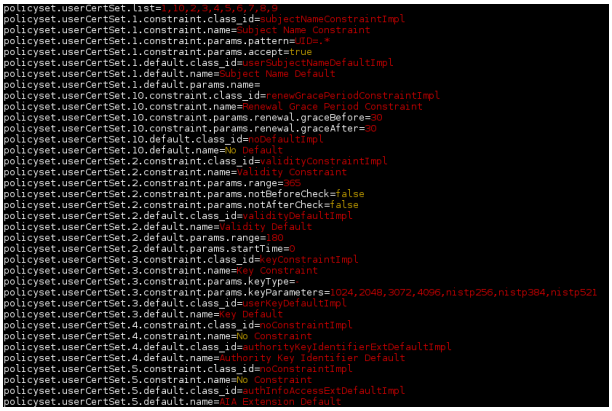


Figure 20: Profile Policies

Last part of the profile is constraints, Policies like:

– validity of the cert
– renewal settings,
– key Usage Extensions

- User supplied extensions

- Publishing Certificate System provides customizable framework from CA's to publish.

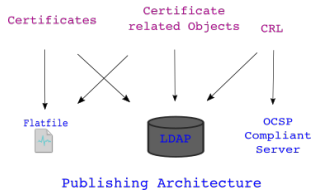


Figure 21: Publishing Architecture

  - Key Features
    - Publish to a single repositories or multiple repositories
    - Split locations by certificates/CRL
    - Set individual rules for each type of certs/crl
  - Publishing framework consists
    - Publishers
    - Mappers
    - Rules
  - Publishers: Publishers specify location to which certificates/CRL's are to be published. Example:
    - To publish to a file, publishers specify the location of the publishing directory.
    - To publish to LDAP, publishers specify the attribute in the directory that srores the cert/CRL.
    - To publish to OCSP, we specify OCSP Server details.
  - Rules: Rules define
    - what is to be published and where ?
    - What type of certs can be published to what location
    - Set rules to publish certs to file and LDAP
    - Set individual rules for each type of cert/rule
    - There are rules for Files, LDAP and OCSP
  - Mappers: Mappers are only used when publishing to LDAP
    - Mappers construct the DN for an entry based on the information from the certificate or certificate request.
    - Mappers use certificate or certificate request's subject name to construct the DN of the entry to which cert/certificate request/CRL has to be published

3.1.7 Exercises

3.2 Key Recovery Authority

3.3 Online Certificate Status Protocol

3.4 Token Key Service & Token Processing System