Tutorial 2

1.Key Exchange

Assume Alice has a (public,private) key pair (e,d). She wants to send her public key to Bob so they can establish a symmetric key based secure channel for sending the message M.

Is the following protocol for this secure (N is a nonce chosen by Alice)?

Alice → Bob: e,N
Bob → Alice: $E_e(k,N)$
Alice → Bob: $E_k(M)$

- Man-in-the-middle attack

Alice→Eve: e,N

Eve→ Bob: e’,N

Bob→Eve: Ee’(k,N)

Eve→ Alice: Ee(k’,N)

Alice→ Eve: Ek’(M)

Eve→ Bob: Ek(M)

So how can we fix it?

Have the public keys signed by a trusted certification authority. Assume the public key of Alice has been signed by a trusted certification authority CA and that the public key of CA is public so anyone (Bob in particular) can check the signature.

CertA = (Alice, e, expirydate,Sig_{CA})

Alice → Bob: CertA, N Bob: Verifies e.
Bob → Alice: E_e(k, N)
Alice → Bob: E_k(M)

Is Bob sure that M was sent by Alice now?

Yes (assuming the M has some appropriate structure)! Although possibly no if it doesn’t. But wait …

Is Alice sure that she is sending M to Bob?

No. ☹

Can we do something here too?

Yes. Assume Bob’s public key e’ is certified by the CA so Bob has a certified certificate CertB. Bob’s private key is d’.

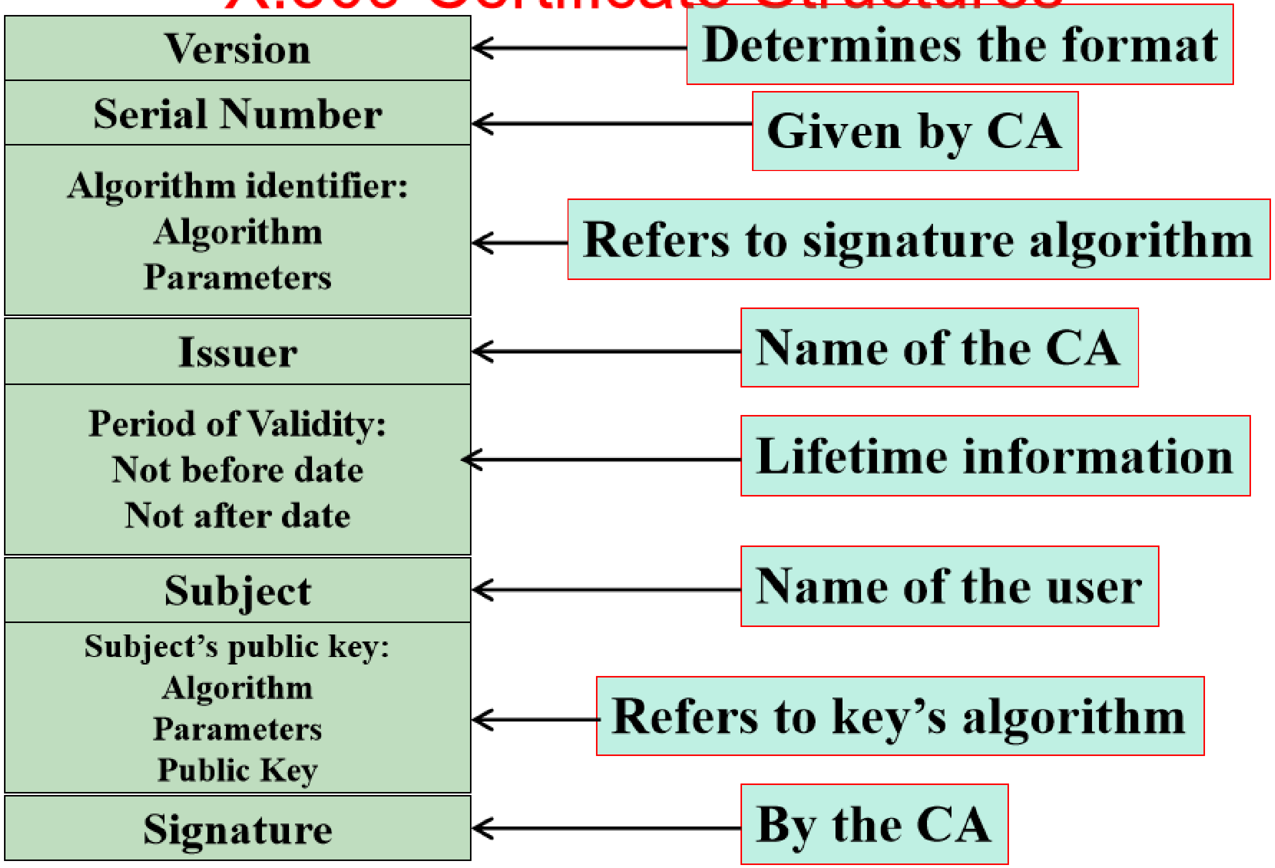
We change the second step on the previous protocol to…

Bob → Alice: CertB, $E_e(k, N, Sig_{d'}(k, N))$

Alice verifies Cert B and $Sig_{d'}(k, N)$ which denotes Bob’s signature.

2. Certificate

X.509 Certificate Structures

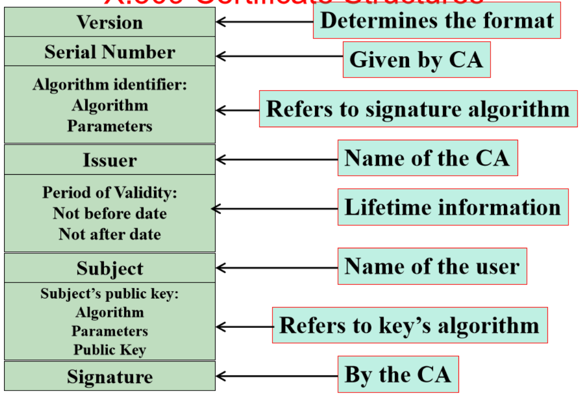


Version	Determines the format
Serial Number	Given by CA
Algorithm identifier: Algorithm Parameters	Refers to signature algorithm
Issuer	Name of the CA
Period of Validity: Not before date Not after date	Lifetime information
Subject	Name of the user
Subject’s public key: Algorithm Parameters Public Key	Refers to key’s algorithm
Signature	By the CA

What will happen if ``Subject” was not included and signed by CA?

2. Certificate

X.509 Certificate Structures



Version	Determines the format
Serial Number	Given by CA
Algorithm identifier: Algorithm Parameters	Refers to signature algorithm
Issuer	Name of the CA
Period of Validity: Not before date Not after date	Lifetime information
Subject	Name of the user
Subject’s public key: Algorithm Parameters Public Key	Refers to key’s algorithm
Signature	By the CA

What will happen if ``Subject” was not included and signed by CA?

- A key pk certified by CA for user hackers.com can be modified into for user UOW. Then clients in the future might talk to hackers.com while they believe that they are talking to UOW.

3.PKI

What do the following terms mean in a general sense, that is, independent of public key infrastructures?

i. Monopoly.

ii. Anarchy.

iii. Oligarchy.

A *Monopoly* is where an individual (or single group) has the means of producing, selling or providing a commodity or service. It is also used in the sense of controlling a market (monopolising a market) to the extent of controlling prices and being able to exclude competition.

Think about Monarchy too, in the sense of a single ruler.

An *oligarchy* is a political system governed by a few. This ties back to rule by aristocracy (in theory the best).

Anarchy is an absence of political *authority.* It corresponds to the lack of any cohesive principle, such as a common standard or purpose. Such states of lawlessness and disorder usually result from a failure of government.

4.PKI

- What distinguishes good-lists and bad-lists for PKI revocation? Why are good-lists more secure?

  Bad-lists show which certificates have been revoked. Good-lists show which certificates are still valid. Good-lists are more secure since the existence of a certificate at generation needs to be made public (in the sense of adding it to the good-list), whereas bad-lists give no indication of how many certificates there are around (i.e. the CA may generate more than one certificates for one user).

5.PKI

Is trust an equivalence relation in PKI’s?

Reflexive : A trusts A ?

Symmetric : A trusts B → B trusts A ?

Transitive : A trusts B,
B trusts C → A trusts C ?

In PKI’s: Yes.

Depends (anarchy versus delegated CA’s).

Depends (anarchy versus delegated CA’s).

6.Anonymous Key?

What does it mean to have anonymous (public, private) key pairs? Is it a useful concept?

- A key pair is associated with an unknown person. It is certainly useful, particularly if the unknown person is anonymous in the sense of their name or identity being unknown but their role being clear. For example, an anonymous referee. You can consistently communicate with a pseudo-identity (the public key essentially).
- As long as the key distribution is not a problem

7.What is Nonce?

In computer security a nonce is a number used once. It is useful in such things as challenges and identifies a session. By recording the nonce’s one can avoid replay attacks.

In using a nonce as a challenge one needs to be sure not to use it twice.

Literally, it means ‘for the present time’, or ‘for a single occasion or purpose’.

8.Time Stamp

Is a timestamp a nonce?

- Yes
- Timestamps require reasonably synchronized clocks

- Read this: https://www.unixtimestamp.com/

9.Sequence Numbers

Are sequence numbers nonces?

- Yes
- Sequence numbers require stability, what happens if there is a restart after a crash?

Nonce

In practice, nonce is generally a very large random number. This number must be sufficiently large (e.g. 80-bit) so that the probability that the number will repeat is negligible.