Digital Certificates simplflied

Digital Certificates are one of the foundation blocks of security in the digital woorld. They are used to authenenticate the identity of the device and secure the tranactions between devices. This section provides a simplflied overview of the digital certificates.

Symmetric key cryptography

In Symmetric key cryptography same key is used to encrypt and decrypt.

- Advantage: They are faster to encrypt and decrypt
- Disadvantage: The secret key has to be distributed between the sender and receiver

Assymmetric key cryptography (public key cryptography)

Assymmetric key cryptography solves the above mentioned key distribution problem with 2 keys (key pair).

- One of the keys is kept scret - private key
- Other key is made public - public key

There are different algorithms used for assymmetric key cryptography.

- RSA
- DSA
- ECC

Some algorithms like RSA technically allows you to choose which key is private and which is public. But some others like ECC does not give you a choice as they are dissimilar in computation. Tools like openssl indicate which key to use as private avoiding any confusions here

Hybrid approach

The Assumetric encryption is computationally heavy as compared to the symmetric encryption. In practical usecases a hybrid approach is used where public key cryptography is used for securely sharing symmetric key. After this initial step, the symmetric key is used always.

Key operations

Sharing

- Public keys can be shared to anyone publicly.
- Private keys are not shared with anyone else

Public keys can be shared via different mechanims . For example:

- Manually via email
- Using TLS

Oneway Encryption

- If public key is used to encrypt the message, only the private key can be used to decrypt the message.
- If private key is used to encrypt the message, only the public key can be used to decrypt the message.

Alice shares public key to rest of the world including Bob. Bob uses it to encrypt data and send to Alice. Alice decrypts with private key. Nobody else can decrypt it since they dont have private key

Jac plays the trick

Jac can get Alice's public key since it is shared to the world. Jac uses Alice's public key and sends Alice a message imperonating Bob "Hi Alice, I am Bob !". Alice will be able to decrypt it her private key. Alice thinks it came from Bob, and may respond to him!

To avoid this, digital signatures are used. Bob signs the message using Bob private key. Alice uses Bobs shared public key to verify the signature always. Now Jac cannot impersonate Bob since Jac dont have Bobs private key to sign the message

Key exchange

Host name verification

References

https://crypto.stackexchange.com/questions/93641/can-we-pick-which-key-is-private-or-public-in-asymmetric-encryption-do-the-keys