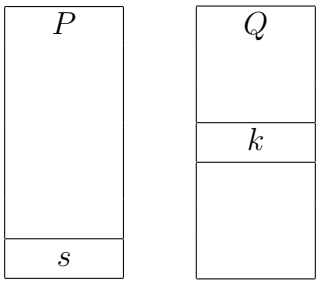
Consider two certificates P and Q where P is signed by Q. Let s be the signature in P and let k be the public key in Q.



Let k' be the secret key associated with k. Only the owner of Q knows the secret key.

Signature s is a hash digest of P encrypted using the secret key k'. For example, here is the signature in ASN notation for a sample certificate P that uses elliptic curve prime256v1 and hash digest sha256.

```
32 bytes INTEGER 1220162783f6e99b72b83a8d886a16def052bb3835e9ecdbd8d526d2b5f75f7c
32 bytes INTEGER 3741f927b410661ef7f2a3b8a669ad03dbe0576d84429efe41dfe0e0c940c1fa
```

To prove that P is signed by Q, signature s is decrypted using Q's public key k. Then if the decrypted value matches the digest of P (sha256 in this example), the signing of P by Q is proven. The contents of P cannot be changed without breaking signature s, and s cannot be changed without knowing the secret key k'. Hence the contents of P can be trusted.