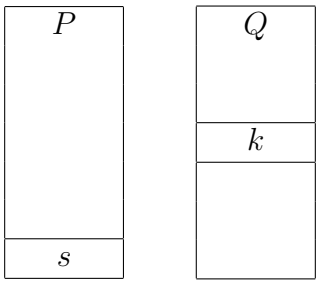
Consider two certificates P and Q where P is signed by Q. Let s be the signature in P and let k be the public key in Q.



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 secret key k'. For example, here is a prime256v1 signature with the TLVs (tag, length, value) decoded.

```
233  72:   BIT STRING, encapsulates {
236  69:     SEQUENCE {
238  32:       INTEGER
       :         79 25 86 F1 40 A1 00 DD 18 B2 18 9A 00 D7 74 D5
       :         51 05 90 7C 5A E4 A6 70 69 EA D8 D8 71 F1 7F 85
272  33:       INTEGER
       :         00 FF 3D AB 62 84 1C C3 35 30 45 41 49 FA 05 CC
       :         A5 BC CC 80 D3 89 EA 96 57 B1 97 F6 D7 63 95 4A
       :         9D
       :       }
       :     }
       :   }
```

The two integers are the encryption result. The second integer is 33 bytes because of the ASN.1 coding rule that the first bit of an integer must be 0. The TLVs are nested such that the two integers are the value of "sequence" and "sequence" is the value of "bit string."

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, 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.