

# External Public Keys

## draft-ounsworth-lamps-pq-external-pubkeys

---

Mike Ounsworth, Markku-Juhani O. Saarinen, John Gray, David Hook.

LAMPS 118



**ENTRUST**

SECURING A WORLD IN MOTION

---

At this time we are **NOT** looking for WG adoption, only socializing this idea.

# Core idea

---

- Where public keys are extremely large (cough cough McEliece), then don't put them in the cert.

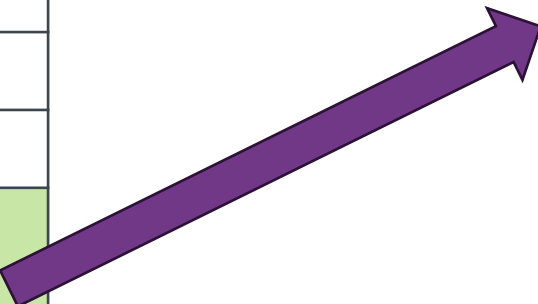
The certificate's subjectPublicKey is the DER encoding of the following structure:

```
ExternalValue ::= SEQUENCE {  
    location      GeneralNames,  
    hashAlg      AlgorithmIdentifier,  
    hashVal      OCTET STRING  
}
```

# Core Idea

Where public keys are extremely large (cough cough McEliece with 0.25 – 1.3 mb pub keys), then don't put them in the cert.

CERTIFICATE
Subject: cn=joe
Issuer: CACorp
Serial: 07
SPKI: { location: http://joe.com/pubkey hash: 8eff38e8... }
Extensions:
SANs: joe.com
Sig: SLH-DSA {a620bf96d6b..}



```
-----BEGIN PUBLIC KEY-----  
MIIBigKAYEAq3DnhgYgLV...  
ar4jRygpzbghlFn0Luk1mdV...  
...  
jXPqy/ZJ/+...  
-----END PUBLIC KEY-----
```

draft-ounsworth-lamps-pq-external-pubkeys:  
The certificate's subjectPublicKey is the DER encoding of the following structure:

```
ExternalValue ::= SEQUENCE {  
    location      GeneralNames,  
    hashAlg       AlgorithmIdentifier,  
    hashVal       OCTET STRING  
}
```



# History of this draft

---

- In March, 2021 Markku suggested “hashed public key for "BSI" KEMTLS” on the LAMPS mail list<sup>1</sup>.
- Markku and I published draft-ounsworth-pq-external-pubkeys-00 at that time.
- It was not well-received and allowed to expire.
- During the Sept 2023 Interim Hackathon, we learned that BouncyCastle has implemented this draft at the request of one of their customers.
- Since it’s being used, we’re reviving it.
  
- Even if Classic McEliece is the only usecase, I think that still justifies the existence of this mechanism.

<sup>5</sup> 1: [lamps] hashed public key for "BSI" KEMTLS: <https://mailarchive.ietf.org/arch/msg/spasm/Jj3coKtNj24gLsIIDtAzSxETAWA/>

