draft-ietf-lamps-private-key-stmt-attr-00

Russ Housley

IETF 122, LAMPS WG

18 March 2025

Statement of Possession of a Private Key

This document specifies an attribute for a statement of possession of a private key by a certificate subject. As part of X.509 certificate enrollment, a Certification Authority (CA) typically demands proof that the subject possesses of the private key that corresponds to the to-be-certified public key. In some cases, a CA might accept a signed statement from the certificate subject. For example, when a certificate subject needs separate certificates for signature and key establishment, a statement that can be validated with the previously issued signature certificate for the same subject might be adequate for subsequent issuance of the key establishment certificate.

The “statement” made by including the attribute

The attribute for statement of possession of a private key is included in a certificate request to make the following statement:

> "The subject of the signature certificate that is used to validate the signature on this certificate request also has possession of the private key that corresponds to the public key in the certificate request."

Two PKCS#10 CSRs to get two certificates

1. The subject generates the signature key pair.
2. The subject composes a PKCS#10 Certificate Signing Request (CSR) in the usual manner. It includes a signature that is produced with the private key from step 1.
3. The subject sends the CSR to the CA, and it gets back a signature certificate. The signature certificate includes a key usage of digitalSignature and/or nonRepudiation.
4. The subject generates the key establishment key pair.
5. The subject composes a PKCS#10 CSR containing the key establishment public key. The CSR attributes include the attribute specified in this document. The subject name matches the one from step 2. The CSR includes a signature that is produced with the private key from step 1.
6. The subject sends the CSR to the CA, and it gets back a key establishment certificate. The key establishment certificate includes a key usage of keyEncipherment or keyAgreement.

Simple ASN.1 Attribute Definition

```
id-at-privateKeyStatement OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 22112 2 1 }

privateKeyStatement ATTRIBUTE ::= {
        TYPE PrivateKeyStatement
        IDENTIFIED BY id-at-privateKeyStatement }

PrivateKeyStatement ::= SEQUENCE {
        signer  IssuerAndSerialNumber,
        cert    Certificate OPTIONAL }
```

Way Forward

- Discussed on the LAMPS WG mail list
- Lead to change in terminology, but no technical changes
- Ready for WG Last Call
  - Of course, Tim will make the consensus call