No Revocation Available for Short-lived X.509 Public Key Certificates

IETF118@Prague, CZ

November 8, 2023

Russ Housley, Joe Mandel and Tomofumi Okubo

Certificate Validity

RFC5280 says…

4.1.2.5. Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.

Introduction

- Short-lived X.509v3 public key certificates has no use of revocation mechanisms due to its extremely short lifespan.
- The "noRevAvail" certificate extension explicitly indicates that a certificate has no revocation information available.
- The ITU-T Recommendation X.509-2019/COR.2-2023 approved in October 2023 allows the usage of noRevAvail for Public Key Certificates.
- Setting proper certificate validity periods are crucial to prevent potential security exploits by attackers.

What does it look like?

noRevAvail Certificate Extension

```
ext-noRevAvail EXTENSION ::= {
  SYNTAX NULL
  IDENTIFIED BY id-ce-noRevAvail
  CRITICALITY { FALSE } }
```

noRevAvail Extension OID

```
id-ce-noRevAvail OBJECT IDENTIFIER ::= { id-ce 56 }
```

Next step!

- The idea is pretty straight forward but any comments or suggestions are welcome.
- Ready for not only WG adoption but all the way to WGLC?
- Thanks!

Links

- draft-housley-lamps-norevavail-01
  - https://datatracker.ietf.org/doc/draft-housley-lamps-norevavail/
- ITU-T Recommendation X.509-2019/COR.2-2023, October 2023
  - Below currently only has approval status. The actual document to be published soon.
  - https://www.itu.int/rec/T-REC-X.509-202310-I!Cor2