A Mechanism for X.509 Certificate Discovery

IETF118@Prague, CZ
November 8, 2023
Tomofumi Okubo, Corey Bonnell and John Gray
Introduction

• The idea of this draft accidentally came out from the IETF116 Hackathon PQC table.
• It is a mechanism that complements draft-ietf-lamps-cert-binding-for-multi-auth-01.
• The purpose of this mechanism includes, but not limited to increase cryptographic agility
• This mechanism can also facilitate the transition to any new type of certificates such as Composite or different key sizes.
• The underlying philosophy of this mechanism is similar to RFC5697 Other Certificates Extension.
SIA Extension, Related Certificate Descriptor

```
id-ad  OBJECT IDENTIFIER ::= { 
    iso(1) identified-organization(3) dod(6) internet(1) 
    security(5) mechanisms(5) pkix(7) ad(48) }

id-ad-certDiscovery OBJECT IDENTIFIER ::= { id-ad TBD }

id-on-relatedCertificateDescriptor OBJECT IDENTIFIER ::= { id-on TBD2 }

on-RelatedCertificateDescriptor OTHER-NAME ::= { 
    RelatedCertificateDescriptor IDENTIFIED BY id-on-relatedCertificateDescriptor 
}

RelatedCertificateDescriptor ::= SEQUENCE { 
    relatedCertificateLocation TravelingName, 
    relatedCertificateSignatureAlgorithm [0] IMPLICIT AlgorithmIdentifier OPTIONAL, 
    relatedCertificatePublicKeyAlgorithm [1] IMPLICIT AlgorithmIdentifier OPTIONAL, 
}
```
Next step!

• Is it useful to signal the validation modes? (e.g. primary fails then go fetch secondary, primary fails then don’t fetch secondary, primary succeeds, then go fetch, primary succeeds, then don’t fetch).

• Please bear in mind that there are many different situations and use cases for PKI in the world (There is no such thing as one-size-fits-all).

• Use cases are currently in the works.

• Any comments and suggestions are greatly appreciated.
Links

• A Mechanism for X.509 Certificate Discovery
  • https://www.ietf.org/id/draft-lamps-okubo-certdiscovery-00.html

• Related Certificates for Use in Multiple Authentications within a Protocol

• Other Certificates Extension
  • https://www.rfc-editor.org/rfc/rfc5697.html

• Composite Signatures For Use In Internet PKI
  • https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/