PQ of the CP

(draft-newton-sidr-policy-qualifiers-01)

Andy Newton,

IETF 86 SIDR

WHY?

"*Typically the rationale for the URI is so that the a CA can satisfy it's legal counsel that potential relying parties have been informed, via the URI, of the presence of a CPS, and that RPs who care can download and read it before making use of the certs issued by the CA.*

Its a CYA mechanism."

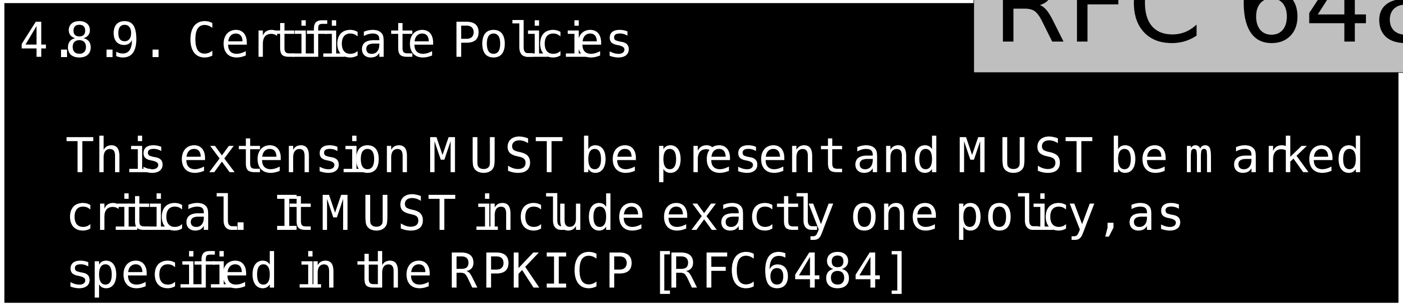
-Steve Kent, 2013-03-05

A Pointer to the CPS

- In the X.509 PKI world, it is quite common to embed pointers into the CertificatePolicy extension as a PolicyQualifier
  - The IETF’s RPKI Certificate Policy (CP) covers the RPKI as a whole
  - Each CA can have a Certification Practices Statement

Current Ambiquity

RFC 6487



```
4.8.9. Certificate Policies

   This extension MUST be present and MUST be marked
   critical. It MUST include exactly one policy, as
   specified in the RPKI CP [RFC6484]
```

- RFC 6487 is ambiguous on PolicyQualifiers
- Required one line fix to two of the validators

-00 to -01

(thanks Sean Turner)

- Language tightened up
  - Only one CP
  - PolicyQualifier can only by a CPS URL. No text
- IANA Considerations
- Security Considerations
  - CPS URL is a potential DoS vector
  - No processing requirement on the CPS URL, just like RFC 5280

Since -01

- "they are a malware attack vector"
  - -01 security considerations state there is no requirement to process the URI
  - Same can be said for every IETF protocol to embed a URI, including current RPKI certs
- "no one ever sees the urls"
  - Then they cannot be an attack vector and are therefore innocuous.