OCSP over DNS

https://datatracker.ietf.org/doc/draft-pala-odin/

Massimiliano Pala <m.pala@cablelabs.com>
CableLabs / OpenCA
The Proposal

• Enable DNS as a distribution mechanism for OCSP responses
Benefits

• Increased the availability of OCSP responses by leveraging the distributed (close-to-the-user) caching of DNS
• Reduced operational costs associated with the distribution of revocation information
• The use of DNSSEC (when available) can help mitigating MITM and Reply attacks (solving the TLS circular reference)
• DNS queries accessible even when HTTP/S is not
• Simplified Query Messages
The (SIMPLE) Gory Details

• RDATA for OCSP RR

```
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

• URL Example for OCSPRR

```
dns://04A3E45534A1B5.ca1.example.com?type=OCSPRR
```
OCSP over DNS: How-To

a. Retrieve the OCSP URI provided in the AIA of the certificate to be checked
b. (If the scheme is “dns://”) retrieve the DNS record carrying the required OCSP response
c. Continue processing the retrieved data according to the OCSP protocol
OCSP over DNS (summary)

• The proposal details (draft-pala-odin-03)
  • OCSP RR Definition
  • Uses existing AIA accessMethod (id-ocsp)
  • DNS URL in certificates

• Benefits
  • Increased availability of Revocation information (closer to the user)
  • Reduced costs for providing revocation services
  • Deployment w/ DNSSEC can provide better security (HTTPS loophole)
  • Simplified query mechanism for applications
Questions and Next Steps

• Does this work belong in existing WG?
• Shall we have a new WG with BoF?
• Shall we have a new WG without BoF?
• AD to sponsor without WG?