Fixing an OID problem in RFC6485

ggm@apnic.net

In RFC 6485 Section 2 the following sentence:

> The Object Identifier (OID) sha256withRSAEncryption from [RFC4055] MUST be used.

Is replaced by:

> One of the Object Identifiers (OID) rsaEncryption or sha256WithRSAEncryption from [RFC4055] MUST be used. RPKI implementations MUST support rsaEncryption for the signatureAlgorithm field and SHOULD support sha256WithRSAEncryption.

All known RPKI CA implementations already do what this draft recommends.

Acknowledgements

Andrew Chi and David Mandelberg discovered this problem.

Russ Housley documented the RFC chain back to 2630.

This draft reflects a discussion between Rob Austein and Matt Lepinski on the SIDR Working group mailing list and a private communication between Rob Austein and Geoff Huston.