7.1.3. Algorithm Object Identifiers

Effective 1 January 2016, CAs MUST NOT issue any new ~~Subscriber certificates or~~ Subordinate CA certificates using the SHA-1 hash algorithm. Effective 1 January 2017, CAs MUST NOT issue any new Subscriber certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. This Section ~~9.4.2~~7.1.3 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

Effective 1 January 2016, CAs MUST NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017. Any SHA-1 Subscriber Certificates issued after 1 January 2016 must be signed by a Subordinate CA certificate with a basicConstraints pathLen=0.