**Appendix F – Issuance of Certificates for .onion Domain Names**

A CA may issue an EV Certificate containing the .onion Domain Name provided that issuance complies with the requirements set forth in this Appendix:

1. CAB Forum Tor Service Descriptor Hash extension (2.23.140.1.31)

The CA MUST include the CAB Forum extension in the TBSCertificate to convey hashes of keys related to .onion addresses. The CA MUST include the Tor Service Descriptor Hash extension using the following format:

cabf-TorServiceDescriptorHash OBJECT IDENTIFIER ::= { 2.23.140.1.31 }

TorServiceDescriptorHash:: = SEQUENCE {

algorithm AlgorithmIdentifier

subjectPublicKeyHash BIT STRING }

Where the AlgorithmIdentifier is a hashing algorithm (defined in RFC 6234) performed over the raw Public Key of the .onion service and SubjectPublicKeyHash is the value of the hash output of the raw Public Key.