Appendix F – Issuance of Certificates for .onion Domain Names

A CA may issue an EV Certificate with .onion in the right-most label of the 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 ~~has created an~~ extension ~~of~~ in the TBSCertificate ~~for use in~~to convey~~ing~~ hashes of keys related to .onion addresses. The CA MUST include the Tor Service Descriptor Hash extension ~~has~~ using the following format:

```
cabf-TorServiceDescriptor OBJECT IDENTIFIER ::= { 2.23.140.1.31 }

TorServiceDescriptorSyntax ::=

    SEQUENCE ( 1..MAX ) of TorServiceDescriptorHash

TorServiceDescriptorHash:: = SEQUENCE {

onionURI                 UTF8String
algorithm                AlgorithmIdentifier
subjectPublicKeyHash     BIT STRING

}
```

Where the AlgorithmIdentifier is a hashing algorithm (defined in RFC 6234) performed over the DER-encoding of an ASN.1 SubjectPublicKey of the .onion service and SubjectPublicKeyHash is the hash output.

2. The CA MUST verify the Applicant's control over the .onion Domain Name using one of the following:

a. The CA MAY verify the Applicant's control over the .onion service by posting a specific value at a well-known URL under RFC5785.

b. The CA MAY verify the Applicant's control over the .onion service by having the Applicant provide a Certificate Request signed using the .onion public key if the Attributes section of the certificationRequestInfo contains:

(i) A caSigningNonce attribute that (1) contains a single value with at least 64-bits of entropy, (2) is generated by the CA, and (3) delivered to the Applicant through a Verified Method of Communication and (ii) An applicantSigningNonce attribute that (1) contains a single value with at least 64-bits of entropy and (2) is generated by the Applicant.

The signing nonce attributes have the following format:

```
caSigningNonce ATTRIBUTE ::= {

WITH SYNTAX                  OCTET STRING
EQUALITY MATCHING RULE       octetStringMatch
SINGLE VALUE                 TRUE
ID                           { cabf-caSigningNonce }

}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {

WITH SYNTAX                   OCTET STRING
EQUALITY MATCHING RULE        octetStringMatch
SINGLE VALUE                  TRUE
ID                            { cabf-applicantSigningNonce }

}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

4. Each Certificate that includes a Domain Name where .onion is in the right-most label of the Domain Name MUST conform to the requirements of these Guidelines, including the content requirements in Section 7.1 of the Baseline Requirements, except that the CA MAY include a wildcard character in the Subject Alternative Name Extension and Subject Common Name Field as the left-most character in the .onion Domain Name provided inclusion of the wildcard character complies with Section 3.2.2.6 of the Baseline Requirements.

5. CAs MUST NOT issue a Certificate that includes a Domain Name where .onion is in the right-most label of the Domain Name with a validity period longer than 15 months.

6. When a certificate that includes a Domain Name where .onion is in the right-most label of the Domain Name, the Domain Name shall not be considered an Internal Name if the Certificate was issued in compliance with this Appendix F.

7. On or before May 1, 2015, each CA MUST revoke all Certificates issued with the Subject Alternative Name extension or Common Name field that includes a Domain Name where .onion is in the right-most label of the Domain Name unless the Certificate was issued in compliance with this Appendix F.