Appendix B – Certificate Extensions (Normative)

This appendix specifies the requirements for Certificate extensions for Certificates generated after the Effective Date.

Root CA Certificate

Root Certificates MUST be of type X.509 v3.

A. basicConstraints

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

B. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

C. certificatePolicies

This extension SHOULD NOT be present.

D. extendedKeyUsage

This extension MUST NOT be present.

All other fields and extensions MUST be set in accordance to RFC 5280.

Subordinate CA Certificate

Subordinate CA Certificates MUST be of type X.509 v3.

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

B. cRLDistributionPoints

This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.

C. authorityInformationAccess

~~With the exception of stapling, which is noted below, t~~This extension MUST be present. It MUST NOT be marked critical, and it MUST contain:

- the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). See Section 13.2.1 for details about OCSP revocation requirements.

- ~~It SHOULD also contain~~ the HTTP URL where a copy of the Issuing (non-Root) CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) can be downloaded from a 24x7 online repository. ~~See Section 13.2.1 for details.~~

~~The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].~~

D. basicConstraints

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

E. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

F. nameConstraints (optional)

If present, this extension SHOULD be marked critical*.

All other fields and extensions MUST be set in accordance to RFC 5280.

* Non-critical Name Constraints are an exception to RFC 5280 that MAY be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide."

Subscriber Certificate

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

- A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

The following extensions MAY be present:

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

B. cRLDistributionPoints

This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service. See Section 13.2.1 for details.

C. authorityInformationAccess

~~With the exception of stapling, which is noted below, t~~This extension MUST be present. It MUST NOT be marked critical, and it MUST contain:

- ~~-~~the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). See Section 13.2.1 for details about OCSP revocation requirements.
- ~~It SHOULD also contain~~ the HTTP URL where a copy of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) can be downloaded from a 24x7 online repository. ~~See Section 13.2.1 for details.~~

~~The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].~~

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

F. extKeyUsage (required)

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present.

All other fields and extensions MUST be set in accordance to RFC 5280.