Appendix A - Cryptographic Algorithm and Key Requirements (Normative)

Certificates MUST meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

	Validity period beginning after 31 Dec 2010	Validity period beginning after 31 Dec 2015
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	2048**
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

(2) Subordinate CA Certificates

	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013	Validity period beginning after 31 Dec 2015
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

(3) Subscriber Certificates

	Validity period ending after 31 Dec 2013	Validity period beginning after 31 Dec 2015
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

*~~-~~Effective immediately CAs SHOULD begin migrating away from using the SHA-1 hashing algorithm to sign Subscriber Certificates. CAs SHOULD advise Applicants that Microsoft has indicated that Windows will stop accepting SHA1 certificates on 1 January 2017 or sooner if the algorithm becomes vulnerable to cryptographic attack.